

Sophos Endpoint Security and Control Guida in linea

Versione prodotto: 10.0

Data documento: dicembre 2011



Sommario

- 1 Informazioni su Sophos Endpoint Security and Control3
- 2 Home page.....4
- 3 Gruppi Sophos.....5
- 4 Sophos Anti-Virus.....8
- 5 Sophos Device Control.....49
- 6 Sophos Data Control.....51
- 7 Sophos Client Firewall.....53
- 8 Sophos AutoUpdate.....82
- 9 Sophos Tamper Protection.....85
- 10 Risoluzione dei problemi.....90
- 11 Glossario.....98
- 12 Supporto tecnico.....104
- 13 Note legali.....105

1 Informazioni su Sophos Endpoint Security and Control

Sophos Endpoint Security and Control, versione 10.0 è una suite di software di sicurezza integrata.

Sophos Anti-Virus rileva e rimuove virus, trojan, worm e spyware, oltre che adware e altre applicazioni potenzialmente indesiderate. La tecnologia HIPS (Host Intrusion Prevention System) può anche proteggere il computer da file sospetto e rootkit.

Sophos Behavior Monitoring utilizza la tecnologia HIPS per proteggere i computer con sistema operativo Windows 2000 e successivo dalle minacce non identificate o del giorno zero, oltre che da comportamento sospetto.

Sophos Live Protection migliora il rilevamento di nuovo malware, senza il rischio di rilevamenti indesiderati. Questo avviene mediante ricerca istantanea in base alle più aggiornate versioni di malware conosciute. Quando viene identificato un nuovo malware, Sophos è in grado di inviare aggiornamenti entro pochi secondi.

Sophos Web Protection fornisce una protezione avanzata contro le minacce del web impedendo l'accesso a percorsi noti per essere host di malware. Blocca l'accesso dei computer a tali siti, mediante la ricerca dei loro dati in tempo reale all'interno del database online Sophos.

Sophos Application Control (controllo applicazioni) blocca applicazioni non autorizzate quali Voice over IP, messaggistica istantanea, condivisione file e software di gioco.

Sophos Device Control (controllo dispositivi) blocca dispositivi di memorizzazione esterni non autorizzati e tecnologie di connessione wireless.

Sophos Data Control (controllo dati) evita la perdita accidentale di dati che possono portare all'identificazione personale da computer gestiti.

Sophos Client Firewall impedisce a worm, trojan e spyware il furto e la distribuzione di informazioni sensibili, oltre che prevenire gli attacchi di pirati informatici.

Sophos AutoUpdate (autoaggiornamento) offre un aggiornamento a prova di errore e il controllo della larghezza di banda quando gli aggiornamenti vengono eseguiti da connessioni di rete a bassa velocità.

Sophos Tamper Protection (blocco rimozione) impedisce a malware noto e utenti non autorizzati (utenti con conoscenze tecniche limitate) la disinstallazione del software di sicurezza Sophos o la disabilitazione tramite l'interfaccia Sophos Endpoint Security and Control.

2 Home page

Quando si apre la finestra di **Sophos Endpoint Security and Control**, nel riquadro a destra viene visualizzata la pagina **Home**. Consente la configurazione e l'utilizzo del software.

Durante l'utilizzo di Sophos Endpoint Security and Control, il contenuto del riquadro a destra cambierà. Per tornare alla **Home** page, cliccare sul pulsante **Home** nella barra degli strumenti.

3 Gruppi Sophos

3.1 Gruppi Sophos

Sophos Endpoint Security and Control limita l'accesso a determinate parti della rete solo ai membri di specifici gruppi Sophos.

Quando viene installato Sophos Endpoint Security and Control, tutti gli utenti del computer vengono inizialmente assegnati a un gruppo Sophos a seconda del gruppo Windows di appartenenza.

Gruppo Windows	Gruppo Sophos
Administrators	SophosAdministrator
Power Users	SophosPowerUser
Utenti	SophosUser

Gli utenti non assegnati ad alcun gruppo Sophos, inclusi gli utenti ospiti, possono svolgere solo le seguenti operazioni:

- Scansione in accesso
- Scansione dal menu del tasto destro del mouse

SophosUsers

I SophosUsers possono svolgere tutte le operazioni riportate qui sopra, oltre a quelle di seguito elencate:

- Apertura della finestra di Sophos Endpoint Security and Control
- Impostazione ed esecuzione delle scansioni su richiesta
- Configurazione della scansione dal menu del tasto destro del mouse
- Gestione, con diritti limitati, degli oggetti in quarantena
- Creazione e configurazione delle regole del firewall

SophosPowerUsers

I SophosPowerUsers hanno gli stessi diritti dei SophosUsers, oltre ai seguenti diritti aggiuntivi:

- Maggiori privilegi nella gestione della quarantena
- Accesso al gestore autorizzazioni

SophosAdministrators

I SophosAdministrators possono utilizzare e configurare qualsiasi parte di Sophos Endpoint Security and Control.

Nota: Se il blocco rimozione è abilitato, un SophosAdministrator deve conoscere la password del blocco rimozione per effettuare le seguenti operazioni:

- Configurazione della scansione in accesso.
- Rilevamento di comportamento sospetto.
- Disabilitare il blocco rimozione

Per ulteriori informazioni, consultare la sezione [Il blocco rimozione in questo computer](#) a pagina 85.

3.2 Aggiunta di utenti al gruppo Sophos

Gli amministratori di dominio o i membri del gruppo Windows Administrators in tale computer possono cambiare il gruppo Sophos a cui appartiene un determinato utente. Solitamente questa operazione viene svolta per modificare i diritti di accesso a Sophos Endpoint Security and Control.

Per aggiungere utenti al gruppo Sophos:

1. Se si utilizza Windows, aprire Gestione computer.
2. Nella struttura ad albero della console, cliccare su **Users**.
3. Cliccare col tasto destro del mouse sull'account utente e poi su **Proprietà**.
4. Nella scheda **Membro di**, cliccare su **Aggiungi**.
5. In **Immettere i nomi degli oggetti da selezionare**, digitare il nome di un gruppo Sophos:
 - **SophosAdministrator**
 - **SophosPowerUser**
 - **SophosUser**
6. Se si desidera convalidare il nome del gruppo Sophos, cliccare su **Controlla nomi**.

La prossima volta che l'utente accederà al computer, i diritti di accesso a Sophos Endpoint Security and Control saranno cambiati.

Note

- Per aprire Gestione computer, cliccare su **Start** e successivamente su **Pannello di controllo**. Cliccare due volte su **Strumenti di amministrazione** e due volte su **Gestione computer**.
- Per rimuovere un utente da un gruppo utenti Sophos, dalla scheda **Membro di**, selezionare il gruppo da **Membro di** e cliccare su **Rimuovi**.

3.3 Configurazione dei diritti utente per il Gestore quarantena

Se si appartiene al gruppo SophosAdministrator, è possibile configurare i diritti utente per il Gestore quarantena.

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Diritti utente per Gestore quarantena**.

2. Selezionare il tipo di utente che svolgerà un certo tipo di azione.

Nota: eccezion fatta per l'opzione **Autorizza**, i diritti qui impostati vengono applicati solo al **Gestore quarantena**.

Opzione	Descrizione
Disinfetta settori	Gli utenti possono disinfettare il boot sector del floppy disk.
Disinfetta file	Gli utenti possono disinfettare documenti e programmi.
Cancella file	Gli utenti possono cancellare file infetti.
Sposta file	Gli utenti possono spostare i file infetti in un'altra cartella.
Autorizza	Gli utenti possono autorizzare oggetti sospetti, adware e PUA, al fine di consentirne l'esecuzione nel computer. Questa opzione è applicabile sia al Gestore autorizzazioni che al Gestore quarantena .

4 Sophos Anti-Virus

4.1 Scansione in accesso e su richiesta

Scansione in accesso

La scansione in accesso rappresenta il principale metodo di protezione contro virus e altre minacce.

Ogni qual volta si copia, sposta o accede a un file, Sophos Anti-Virus ne esegue la scansione e ne consente l'accesso solo se tale file non costituisce una minaccia per il computer o se autorizzato per l'utilizzo.

Gli Amministratori Sophos possono in aggiunta impostare l'esecuzione della scansione dei file quando essi vengono salvati, creati o rinominati.

Per ulteriori informazioni, consultare la sezione [Configurazione della scansione in accesso](#) a pagina 8.

Scansione su richiesta

La scansione su richiesta fornisce ulteriore protezione. Come intuibile dal nome, è l'utente che avvia la scansione su richiesta. È possibile eseguire una scansione di tutto, da un file singolo all'intero computer.

Per ulteriori informazioni, consultare la sezione [Tipi di scansione su richiesta](#) a pagina 15.

4.2 Scansione in accesso

4.2.1 Scansione in accesso

Si consiglia l'utilizzo delle impostazioni predefinite per la scansione in accesso, per ottenere il giusto equilibrio fra la protezione dei computer dalle minacce e la resa del sistema.

Nota: La scansione in accesso potrebbe non rilevare i virus, se sono installati determinati software di cifratura. Modificare i processi di avvio per assicurarsi che i file vengano decifrati quando inizia la scansione in accesso. Per ulteriori informazioni su come utilizzare criteri antivirus e HIPS con software di cifratura, consultare l'articolo 12790 della knowledge base Sophos (<http://www.sophos.com/support/knowledgebase/article/12790.html>, in inglese).

4.2.2 Configurazione della scansione in accesso

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Per impostazione predefinita, Sophos Anti-Virus rileva e disinfetta le seguenti minacce durante la scansione in accesso:

- virus
- trojan

- worm
- Spyware

Per configurare la scansione in accesso:

1. Cliccare su **Inizio > Anti-virus e HIPS (Sistema di prevenzione delle intrusioni su host) > Configurazione di antivirus e HIPS > Configurazione > scansione in accesso scansione**.
2. Per apportare modifiche alla tempistica in cui viene eseguita la scansione in accesso, in **Verifica file in**, impostare le opzioni secondo quanto descritto qui di seguito.

Opzione	Descrizione
Lettura	Scansione dei file quando copiati, spostati o aperti.
Rinomina	Scansione dei file quando rinominati.
Scrittura	Scansione dei file quando salvati o creati.

3. In **Esegui scansione alla ricerca di**, impostare le opzioni come descritto di seguito.

Opzione	Descrizione
Adware e PUA	L'adware prevede la presentazione all'utente di messaggi pubblicitari, quali messaggi popup, che possono incidere sulla produttività degli utenti e sull'efficienza del sistema. I PUA (Potentially Unwanted Applications) non sono malevoli, ma inadatti a reti aziendali e ambienti lavorativi.
File sospetti	I file sospetti presentano una serie di caratteristiche comunemente, ma non esclusivamente, riscontrate in virus.

4. In **Altre opzioni di scansione**, impostare le opzioni come descritto di seguito.

Opzione	Descrizione
Accesso alle unità con settore di avvio infetti	<p>Attivare questa opzione per consentire l'accesso a uno mezzo o dispositivo rimovibile infetto, quale CD di avvio, floppy disk o unità flash USB.</p> <p>Utilizzate questa opzione soltanto su consiglio del supporto tecnico di Sophos.</p> <p>Consultare anche l'argomento Accesso alle unità con settore di avvio infetti a pagina 94 nella sezione <i>Risoluzione dei problemi</i>.</p>
Scansione di tutti i file	<p>Si consiglia di eseguire la scansione di tutti i file solo durante la scansione settimanale; la scansione di tutti i file limita le prestazioni del computer.</p>
Scansione dei file di archivio	<p>Abilitare questa opzione per eseguire la scansione del contenuto dei file di archivio o compressi prima che venga scaricato o inviato per e-mail dal computer.</p> <p>Si consiglia di lasciare questa opzione disabilitata, dal momento che rallenta notevolmente la scansione.</p> <p>Si sarà comunque protetti da eventuali minacce presenti nei file di archivio o compressi, dal momento che tutti i componenti dei file di archivio o compressi che potrebbero contenere malware verranno bloccati dalla scansione in accesso:</p> <ul style="list-style-type: none"> ■ Quando si apre un file estratto dal file di archivio, tale file viene sottoposto a scansione. ■ I file compressi tramite utilità di compressione dinamiche, quali PKLite, LZEXE e Diet, vengono sottoposti a scansione.
Scansione della memoria di sistema	<p>Abilitare questa opzione per seguire automaticamente una scansione di background a cadenza oraria per rilevare malware nascosti nella memoria di sistema del computer (la memoria utilizzata dal sistema operativo).</p>

4.2.3 Disabilitazione temporanea della scansione in accesso

Se si appartiene al gruppo SophosAdministrator, può presentarsi la necessità di disabilitare temporaneamente la scansione in accesso per motivi di manutenzione o per la risoluzione di alcuni problemi e successivamente di riabilitarla. È possibile disabilitare la protezione in accesso, ma continuare ad eseguire scansioni su richiesta del computer.

Sophos Endpoint Security and Control conserva le impostazioni scelte in questa pagina, anche dopo il riavvio del computer. Se si disabilita la scansione in accesso, il computer risulta non protetto finché la scansione in accesso non venga riabilitata.

1. Cliccare su **Inizio > Anti-virus e HIPS (Sistema di prevenzione delle intrusioni su host) > Configurazione di antivirus e HIPS > Configurazione > scansione in accesso scansione**.
2. Deselezionare la casella di spunta **Consenti scansione in accesso per questo computer**.

4.2.4 Configurazione della disinfezione in accesso

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Per configurare la disinfezione in accesso:

1. Cliccare su **Inizio > Anti-virus e HIPS (Sistema di prevenzione delle intrusioni su host) > Configurazione di antivirus e HIPS > Configurazione > scansione in accesso scansione**.
2. Cliccare sulla scheda **Disinfezione**.
3. Per disinfettare automaticamente gli oggetti infetti, in **Virus/spyware**, selezionare la casella di spunta **Disinfetta automaticamente gli oggetti contenenti virus o spyware**.

Nota: Se si seleziona tale opzione, la disinfezione di virus/spyware darà inizio a una scansione completa del sistema, che cercherà di rimuovere dal computer *tutti* i virus. Ciò potrebbe richiedere molto tempo.

4. In **Viruses/spyware**, selezionare l'azione che Sophos Anti-Virus dovrà intraprendere contro gli oggetti infetti, nel caso la disinfezione automatica sia stata disabilitata o non riesca:

Opzione	Descrizione
Nega solo l'accesso	Sophos Anti-Virus chiede quale azione intraprendere prima di continuare. Si tratta di un'impostazione predefinita.
Cancella Nega l'accesso e sposta in	Utilizzate queste impostazioni soltanto su consiglio del supporto tecnico di Sophos. Utilizzare altrimenti il Quarantine Manager per disinfettare il computer dai virus e spyware rilevati da Sophos Anti-Virus . Consultare la sezione Gestione di virus e spyware in quarantena a pagina 37.

5. In **File sospetti**, selezionare l'azione che Sophos Anti-Virus intraprenderà al rilevare file contenenti codici utilizzati comunemente da malware:

Opzione	Descrizione
Nega l'accesso	Sophos Anti-Virus chiede quale azione intraprendere prima di continuare. Si tratta di un'impostazione predefinita.
Cancella Nega l'accesso e sposta in	Utilizzate queste impostazioni soltanto su consiglio del supporto tecnico di Sophos. Utilizzare invece il Quarantine Manager per disinfettare il computer dai file sospetti rilevati da Sophos Anti-Virus. Consultare la sezione Gestione di file sospetti in quarantena a pagina 39

4.2.5 Ripristino dei file checksum scansionati

L'elenco dei file checksum scansionati viene ripristinato quando viene eseguito un aggiornamento di Sophos Anti-Virus, oppure quando viene riavviato il computer. L'elenco viene ricostruito con i nuovi dati mano a mano che i file vengono scansionati da Sophos Anti-Virus.

È possibile ripristinare l'elenco di file checksum scansionati da Sophos Endpoint Security and Control, se non si desidera riavviare il computer.

Per ripristinare i file checksum scansionati:

1. Cliccare su **Inizio > Anti-virus e HIPS (Sistema di prevenzione delle intrusioni su host) > Configurazione di antivirus e HIPS > Configurazione > scansione in accesso scansione**.
2. Nella scheda **Scansione**, cliccare su **Pulisci cache**.

4.2.6 Specificazione delle estensioni dei file per la scansione in accesso

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

È possibile specificare quali estensioni dei file debbano essere verificate durante la scansione in accesso.

1. Cliccare su **Inizio > Anti-virus e HIPS (Sistema di prevenzione delle intrusioni su host) > Configurazione di antivirus e HIPS > Configurazione > scansione in accesso scansione**.
2. Cliccare sulla scheda **Estensioni** ed impostare le opzioni secondo quanto descritto di seguito.

Scansione di tutti i file

Cliccare su questa opzione per abilitare la scansione di tutti i file, indipendentemente dall'estensione del file.

Consenti scelta delle estensioni da esaminare

Cliccare su questa opzione per restringere la scansione ai soli file con un'estensione particolare, specificata nella lista delle estensioni.



Attenzione: l'elenco delle estensioni include i tipi di file che Sophos consiglia di esaminare. Fare attenzione se si modifica l'elenco secondo quanto descritto di seguito.

Per aggiungere un'estensione alla lista, cliccare su **Aggiungi**. È possibile utilizzare il carattere jolly "?" al posto di un singolo carattere.

Per rimuovere un'estensione dalla lista, selezionare l'estensione e cliccare su **Rimuovi**.

Per modificare un'estensione nella lista, selezionare l'estensione e cliccare su **Modifica**.

Selezionando **Consenti scelta delle estensioni da esaminare**, l'opzione **Scansione dei file senza estensione** viene selezionata per impostazione predefinita. Per disabilitare la scansione dei file senza estensione, deselegionare **Scansione dei file senza estensione**.

4.2.7 Aggiunta, modifica o cancellazione delle esclusioni per la scansione in accesso

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Per modificare l'elenco di file, cartelle e unità esclusi dalla scansione in accesso:

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Scansione in accesso** .
2. Cliccare sulla scheda **Esclusioni**, quindi scegliere una delle seguenti opzioni.
 - Per specificare file, cartelle o unità che si desidera escludere da una scansione in accesso, cliccare su **Aggiungi**.
 - Per cancellare un'esclusione, cliccare su **Rimuovi**.
 - Per modificare un'esclusione, cliccare su **Modifica**.
3. Per aggiungere o modificare un oggetto escluso, nella finestra di dialogo **Escludi oggetto**, selezionare **Tipo di oggetto**.
4. Specificare il **Nome dell'oggetto** utilizzando il pulsante **Sfogli** o digitandolo nella casella di testo.

Nota: se si lavora su una piattaforma a 64 bit, nella finestra di dialogo **Escludi oggetto** il pulsante **Sfogli** non è visibile.

Per ulteriori informazioni su come specificare i nomi degli oggetti, consultare la sezione [Come specificare nomi file e percorsi degli oggetti esclusi dalla scansione](#) a pagina 17.

4.2.8 Come specificare nomi file e percorsi degli oggetti esclusi dalla scansione

Convenzioni di nomenclatura standard

Sophos Anti-Virus convalida i nomi di percorsi e file degli oggetti che si desidera escludere dalla scansione, in base alle convenzioni di denominazione di Windows. Per esempio, il nome di una cartella può contenere spazi, ma non **solo** spazi.

Esclusione di un file specifico

Specificare sia il nome di percorso che file per poter escludere un determinato file. Il percorso può includere una lettera unità o il nome di una condivisione di rete.

C:\Documents\CV.doc

\\Server\Users\Documents\CV.doc

Nota: Per assicurarsi che le esclusioni vengano applicate correttamente, aggiungere nome file e cartella sia nella versione estesa che conforme a 8.3:

C:\Programmi\Sophos\Sophos Anti-Virus

C:\Progra~1\Sophos\Sophos~1

Per ulteriori informazioni, consultare la sezione

<http://www.sophos.com/support/knowledgebase/article/13045.html>.

Esclusione di tutti i file con lo stesso nome

Indicare il nome di un file senza percorso per escludere tutti i file aventi lo stesso nome ovunque si trovino nel file system:

spacer.gif

Esclusione di tutti gli oggetti nell'unità o condivisione di rete

Per escludere tutti gli oggetti contenuti in un'unità o condivisione di rete, indicare la lettera dell'unità o il nome della condivisione:

C:

\\Server

Esclusione di una determinata cartella

Indicare il percorso di una cartella che comprenda una lettera unità o il nome di una condivisione di rete, per escludere tutti gli oggetti presenti in quella cartella e nelle relative sottocartelle:

D:\Tools\logs

Esclusione di tutte le cartelle con lo stesso nome

Indicare il percorso di una cartella senza alcuna lettera unità o nome di condivisione di rete, per escludere qualsiasi oggetto presente in quella cartella e nelle relative sottocartelle in **tutte** le unità o condivisioni di rete. Per esempio, \Tools\logs esclude le seguenti cartelle:

C:\Tools\logs

\\Server\Tools\logs

Nota: È necessario indicare tutto il percorso fino alla lettera unità o al nome della condivisione di rete. Nell'esempio riportato di sopra, indicare \logs non esclude alcun file.

? e caratteri jolly *

Utilizzare il carattere jolly ? nel nome file o estensione al posto di un singolo carattere.

Alla fine di un nome file o estensione, il carattere jolly ? sostituisce un singolo carattere o nessun carattere: per es. file?.txt può indicare i file file.txt, file1.txt e file12.txt, ma non file123.txt.

Utilizzare il carattere jolly * in un nome file o estensione, nel formato [nome file].* o *.[estensione]:

Corretto

file.*

*.txt

Errato

file*.txt

file.txt*

file.*txt

Estensioni file multiple

Nei nomi file con estensioni multiple, l'ultima estensione viene considerata come estensione e le altre come parte del nome:

MySample.txt.doc = nome file MySample.txt + estensione .doc.

4.2.9 Abilitazione del monitoraggio del comportamento

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Se parte del gruppo SophosAdministrator è possibile abilitare il monitoraggio del comportamento.

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Monitoraggio del comportamento**.
2. Nella finestra di dialogo **Configura monitoraggio del comportamento**, mettere la spunta nella casella **Abilita monitoraggio del comportamento**.

4.3 Scansione su richiesta

4.3.1 Tipi di scansione su richiesta

Scansione dal menu del tasto destro del mouse

Esegue in qualsiasi momento la scansione di file, cartelle o unità in Windows Explorer.

- [Esecuzione della scansione dal menu del tasto destro del mouse](#) a pagina 21

Scansione personalizzata

Esegue la scansione di set di file o cartelle specifici. È possibile eseguire una scansione personalizzata sia manualmente, sia pianificandone un'esecuzione autonoma.

- [Esecuzione di una scansione personalizzata](#) a pagina 26
- [Pianificazione di una scansione personalizzata](#) a pagina 25

Scansione completa del computer

Esegue in qualsiasi momento la scansione dell'intero computer, incluso il boot sector e la memoria di sistema.

- [Esecuzione della scansione completa del computer](#) a pagina 27

4.3.2 Specificazione delle estensioni dei file per la scansione su richiesta

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

È possibile specificare quali estensioni dei file debbano essere verificate durante la scansione su richiesta.

1. Dal menu **Configura**, cliccare su **Estensioni ed esclusioni su richiesta**.
2. Cliccare sulla scheda **Estensioni** ed impostare le opzioni secondo quanto descritto di seguito.

Scansione di tutti i file

Cliccare su questa opzione per abilitare la scansione di tutti i file, indipendentemente dall'estensione del file.

Consenti scelta delle estensioni da esaminare

Cliccare su questa opzione per restringere la scansione ai soli file con un'estensione particolare, specificata nella lista delle estensioni.



Attenzione: l'elenco delle estensioni include i tipi di file che Sophos consiglia di esaminare. Fare attenzione se si modifica l'elenco secondo quanto descritto di seguito.

Per aggiungere un'estensione alla lista, cliccare su **Aggiungi**. È possibile utilizzare il carattere jolly "?" al posto di un singolo carattere.

Per rimuovere un'estensione dalla lista, selezionare l'estensione e cliccare su **Rimuovi**.

Per modificare un'estensione nella lista, selezionare l'estensione e cliccare su **Modifica**.

Selezionando **Consenti scelta delle estensioni da esaminare**, l'opzione **Scansione dei file senza estensione** viene selezionata per impostazione predefinita. Per disabilitare la scansione dei file senza estensione, deselezionare **Scansione dei file senza estensione**.

4.3.3 Aggiunta, modifica o cancellazione delle esclusioni per la scansione su richiesta

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

La procedura descritta qui sotto si riferisce a **tutte** le scansioni su richiesta. Per informazioni su come escludere determinati oggetti da una scansione personalizzata, consultare la sezione [Creazione di una scansione personalizzata](#) a pagina 21.

Per modificare l'elenco di file, cartelle e unità esclusi dalla scansione su richiesta:

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Estensioni ed esclusioni su richiesta**.

2. Cliccare sulla scheda **Esclusioni**, quindi scegliere na delle seguenti opzioni.
 - Per specificare file, cartelle o unità che si desidera escludere da una scansione su richiesta, cliccare su **Aggiungi**.
 - Per cancellare un'esclusione, cliccare su **Rimuovi**.
 - Per modificare un'esclusione, cliccare su **Modifica**.
3. Per aggiungere o modificare un oggetto escluso, nella finestra di dialogo **Escludi oggetto**, selezionare il **Tipo di oggetto**.
4. Specificare il **Nome dell'oggetto** utilizzando il pulsante **Sfoggia** o digitandolo nella casella di testo.

Nota: se si lavora su una piattaforma a 64 bit, nella finestra di dialogo **Escludi oggetto** il pulsante **Sfoggia** non è visibile.

Per ulteriori informazioni su come specificare i nomi degli oggetti, consultare la sezione [Come specificare nomi file e percorsi degli oggetti esclusi dalla scansione](#) a pagina 17.

4.3.4 Come specificare nomi file e percorsi degli oggetti esclusi dalla scansione

Convenzioni di nomenclatura standard

Sophos Anti-Virus convalida i nomi di percorsi e file degli oggetti che si desidera escludere dalla scansione, in base alle convenzioni di denominazione di Windows. Per esempio, il nome di una cartella può contenere spazi, ma non **solo** spazi.

Esclusione di un file specifico

Specificare sia il nome di percorso che file per poter escludere un determinato file. Il percorso può includere una lettera unità o il nome di una condivisione di rete.

C:\Documents\CV.doc

\\Server\Users\Documents\CV.doc

Nota: Per assicurarsi che le esclusioni vengano applicate correttamente, aggiungere nome file e cartella sia nella versione estesa che conforme a 8.3:

C:\Programmi\Sophos\Sophos Anti-Virus

C:\Progra~1\Sophos\Sophos~1

Per ulteriori informazioni, consultare la sezione

<http://www.sophos.com/support/knowledgebase/article/13045.html>.

Esclusione di tutti i file con lo stesso nome

Indicare il nome di un file senza percorso per escludere tutti i file aventi lo stesso nome ovunque si trovino nel file system:

spacer.gif

Esclusione di tutti gli oggetti nell'unità o condivisione di rete

Per escludere tutti gli oggetti contenuti in un'unità o condivisione di rete, indicare la lettera dell'unità o il nome della condivisione:

C:

\\Server

Esclusione di una determinata cartella

Indicare il percorso di una cartella che comprenda una lettera unità o il nome di una condivisione di rete, per escludere tutti gli oggetti presenti in quella cartella e nelle relative sottocartelle:

D:\Tools\logs

Esclusione di tutte le cartelle con lo stesso nome

Indicare il percorso di una cartella senza alcuna lettera unità o nome di condivisione di rete, per escludere qualsiasi oggetto presente in quella cartella e nelle relative sottocartelle in **tutte** le unità o condivisioni di rete. Per esempio, \Tools\logs esclude le seguenti cartelle:

C:\Tools\logs

\\Server\Tools\logs

Nota: È necessario indicare tutto il percorso fino alla lettera unità o al nome della condivisione di rete. Nell'esempio riportato di sopra, indicare \logs non esclude alcun file.

? e caratteri jolly *

Utilizzare il carattere jolly ? nel nome file o estensione al posto di un singolo carattere.

Alla fine di un nome file o estensione, il carattere jolly ? sostituisce un singolo carattere o nessun carattere: per es. file?.txt può indicare i file file.txt, file1.txt e file12.txt, ma non file123.txt.

Utilizzare il carattere jolly * in un nome file o estensione, nel formato [nome file].* o *. [estensione]:

Corretto

file.*

*.txt

Errato

file*.txt

file.txt*

file.*txt

Estensioni file multiple

Nei nomi file con estensioni multiple, l'ultima estensione viene considerata come estensione e le altre come parte del nome:

MySample.txt.doc = nome file MySample.txt + estensione .doc.

4.3.5 Scansione dal menu del tasto destro del mouse

4.3.5.1 Configurazione della scansione dal menu del tasto destro del mouse

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa *non* potrà ignorare le modifiche qui apportate.

Per impostazione predefinita, Sophos Anti-Virus rileva e disinfetta le seguenti minacce durante la scansione dal menu del tasto destro del mouse:

- virus
- trojan
- worm
- Spyware
- adware e altre applicazioni potenzialmente indesiderate (PUA)

Per configurare la scansione da menu del tasto destro del mouse:

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Scansione dal menu del tasto destro del mouse**.
2. In **Esegui scansione alla ricerca di**, impostare le opzioni come descritto di seguito.

Opzione	Descrizione
Adware e PUA	L'adware prevede la presentazione all'utente di messaggi pubblicitari, quali messaggi popup, che possono incidere sulla produttività degli utenti e sull'efficienza del sistema. I PUA (Potentially Unwanted Applications) non sono malevoli, ma inadatti a reti aziendali e ambienti lavorativi.
File sospetti	I file sospetti presentano una serie di caratteristiche comunemente, ma non esclusivamente, riscontrate in virus.

3. In **Altre opzioni di scansione**, impostare le opzioni come descritto di seguito.

Opzione	Descrizione
Scansione di tutti i file	Si consiglia di eseguire la scansione di tutti i file solo durante la scansione settimanale; la scansione di tutti i file limita le prestazioni del computer.
Scansione dei file di archivio	<p>Abilitare questa opzione per eseguire la scansione del contenuto dei file di archivio o compressi prima che venga scaricato o inviato per e-mail dal computer.</p> <p>Si consiglia di lasciare questa opzione disabilitata, dal momento che rallenta notevolmente la scansione.</p> <p>Si sarà comunque protetti da eventuali minacce presenti nei file di archivio o compressi, dal momento che tutti i componenti dei file di archivio o compressi che potrebbero contenere malware verranno bloccati dalla scansione in accesso:</p> <ul style="list-style-type: none"> ■ Quando si apre un file estratto dal file di archivio, tale file viene sottoposto a scansione. ■ I file compressi tramite utilità di compressione dinamiche, quali PKLite, LZEXE e Diet, vengono sottoposti a scansione.

4.3.5.2 Configurazione della disinfezione dal menu del tasto destro del mouse

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Per configurare la disinfezione dal menu del tasto destro del mouse:

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Scansione dal menu del tasto destro del mouse**.
2. Cliccare sulla scheda **Disinfezione**.
3. Per disinfettare automaticamente gli oggetti infetti, in **Virus/spyware**, selezionare la casella di spunta **Disinfetta automaticamente gli oggetti contenenti virus o spyware**.
4. Selezionare l'azione che Sophos Anti-Virus dovrà intraprendere contro gli oggetti infetti, nel caso la disinfezione automatica non sia stata abilitata o non riesca:

Opzione	Descrizione
Solo log	<p>Sophos Anti-Virus si limita a registrare gli oggetti infetti nel log della scansione. Consultare la sezione Visualizzazione del log della scansione a pagina 48.</p> <p>Si tratta di un'impostazione predefinita.</p>
Cancella Sposta in	<p>Utilizzate queste impostazioni soltanto su consiglio del supporto tecnico di Sophos.</p> <p>Utilizzare altrimenti il Quarantine Manager per disinfettare il computer dai virus e spyware rilevati da Sophos Anti-Virus. Consultare la sezione Gestione di virus e spyware in quarantena a pagina 37.</p>

5. In **File sospetti**, selezionare l'azione che Sophos Anti-Virus intraprenderà al rilevare file contenenti codici utilizzati comunemente da malware:

Opzione	Descrizione
Solo log	Sophos Anti-Virus si limita a registrare gli oggetti infetti nel log della scansione. Si tratta di un'impostazione predefinita.
Cancella Sposta in	Utilizzate queste impostazioni soltanto su consiglio del supporto tecnico di Sophos. Utilizzare altrimenti il Quarantine Manager per disinfettare il computer dai virus e spyware rilevati da Sophos Anti-Virus . Consultare la sezione Gestione di file sospetti in quarantena a pagina 39

6. Per rimuovere i componenti conosciuti di adware e Potentially Unwanted Applications (PUA) dai computer di tutti gli utenti, in **Adware e PUA**, selezionare la casella di spunta **Disinfetta automaticamente adware e PUA**.

La rimozione non annulla le modifiche già apportate da adware o PUA.

- Per informazioni su come visionare nel sito web di Sophos gli effetti collaterali di adware o PUA, consultare la sezione [Informazioni sulla disinfezione](#) a pagina 43.
- Per informazioni su come disinfettare il computer da adware e PUA utilizzando il Quarantine Manager, consultare la sezione [Gestione di adware e PUA in quarantena](#) a pagina 38 .

4.3.5.3 Esecuzione della scansione dal menu del tasto destro del mouse

È possibile esaminare file, cartelle e unità da Windows Explorer o dal computer eseguendo la scansione dal menu del tasto destro del mouse.

1. Utilizzando Windows Explorer o nel computer, selezionare il file, la cartella o l'unità disco che si desidera scansionare.
È possibile selezionare file e cartelle multipli.
2. Cliccare col tasto destro del mouse sull'oggetto selezionato e successivamente cliccare su **Scansione con Sophos Anti-Virus** .

Se vengono rilevate minacce o applicazioni controllate, cliccare su **Dettagli** e consultare la sezione [Gestione degli oggetti in quarantena](#) della Guida in linea.

4.3.6 Scansioni personalizzate

4.3.6.1 Creazione di una scansione personalizzata

1. Nella **Home** page, sotto **Antivirus e HIPS**, cliccare su **Scansioni**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Cliccare su **Imposta una nuova scansione**.
3. Nel campo di testo **Nome scansione**, digitare un nome per la scansione.

- Nel riquadro **Oggetti da esaminare**, selezionare le unità e le cartelle che si desidera esaminare. A questo scopo, spuntare la casella alla sinistra di ogni unità o cartella. Per informazioni sulle icone visualizzate accanto alle caselle, consultare [Simboli degli oggetti da esaminare](#) a pagina 22.

Nota: le unità o le cartelle non disponibili (perché non sono in linea o sono state cancellate) vengono visualizzate con un carattere barrato. Vengono rimosse dal riquadro **Oggetti da esaminare** se vengono deselezionate o se si apporta una modifica alla selezione della o delle unità o cartelle madri.

- Per configurare ulteriormente la scansione, cliccare su **Configura scansione** (per ulteriori informazioni, consultare la sezione [Configurazione di una scansione personalizzata](#) a pagina 22).
- Per pianificare la scansione, cliccare su **Pianifica scansione**. (per ulteriori informazioni, consultare la sezione [Pianificazione di una scansione personalizzata](#) a pagina 25).
- Cliccare su **Salva** per salvare la scansione oppure **Salva e avvia** per salvare e avviare la scansione.

4.3.6.2 Simboli degli oggetti da esaminare

Nel riquadro **Oggetti da esaminare**, nella casella accanto a ciascun oggetto (unità o cartella) vengono visualizzate diverse icone, a seconda degli oggetti da esaminare. Queste icone sono raffigurate e descritte qui sotto.

Icona	Descrizione
<input type="checkbox"/>	L'oggetto e relativi sotto-oggetti <i>non</i> sono selezionati per la scansione.
<input checked="" type="checkbox"/>	L'oggetto e relativi sotto-oggetti <i>sono</i> selezionati per la scansione.
<input checked="" type="checkbox"/>	L'oggetto è parzialmente selezionato: non l'oggetto in sé ma alcuni suoi sotto-oggetti sono selezionati per la scansione.
<input checked="" type="checkbox"/>	L'oggetto e relativi sotto-oggetti sono esclusi da questa specifica scansione.
<input checked="" type="checkbox"/>	L'oggetto è parzialmente escluso: l'oggetto è selezionato ma alcuni suoi sotto-oggetti sono esclusi da questa particolare scansione.
<input checked="" type="checkbox"/>	L'oggetto e relativi sotto-oggetti sono esclusi da tutte le scansioni su richiesta, perché è stata impostata un'esclusione su richiesta. Per informazioni, consultare la sezione Aggiunta, modifica o cancellazione delle esclusioni per la scansione in accesso a pagina 13.

4.3.6.3 Configurazione di una scansione personalizzata

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Per impostazione predefinita, Sophos Anti-Virus rileva e disinfecta le seguenti minacce durante la scansione personalizzata:

- virus
- trojan

- worm
- Spyware
- adware e altre applicazioni potenzialmente indesiderate (PUA)
- Rootkit

Per configurare una scansione personalizzata:

1. Nella **Home** page, sotto **Antivirus e HIPS**, cliccare su **Scansioni**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nell'elenco **Scansioni disponibili**, selezionare la scansione che si desidera modificare e poi cliccare su **Modifica**.
3. Cliccare su **Configura scansione**.
4. In **Esegui scansione alla ricerca di**, impostare le opzioni come descritto di seguito.

Opzione	Descrizione
Adware e PUA	L'adware prevede la presentazione all'utente di messaggi pubblicitari, quali messaggi popup, che possono incidere sulla produttività degli utenti e sull'efficienza del sistema. I PUA (Potentially Unwanted Applications) non sono malevoli, ma inadatti a reti aziendali e ambienti lavorativi.
File sospetti	I file sospetti presentano una serie di caratteristiche comunemente, ma non esclusivamente, riscontrate in virus.
Rootkit	Se membri del gruppo SophosAdministrator, la scansione alla ricerca di rootkit viene sempre eseguita ogni qual volta si esegua una scansione completa del computer. È possibile eseguire la scansione alla ricerca di rootkit come parte di una scansione personalizzata.

5. In **Altre opzioni di scansione**, impostare le opzioni come descritto di seguito.

Opzione	Descrizione
Scansione di tutti i file	Si consiglia di eseguire la scansione di tutti i file solo durante la scansione settimanale; la scansione di tutti i file limita le prestazioni del computer.
Scansione dei file di archivio	<p>Abilitare questa opzione per eseguire la scansione del contenuto dei file di archivio o compressi prima che venga scaricato o inviato per e-mail dal computer.</p> <p>Si consiglia di lasciare questa opzione disabilitata, dal momento che rallenta notevolmente la scansione.</p> <p>Si sarà comunque protetti da eventuali minacce presenti nei file di archivio o compressi, dal momento che tutti i componenti dei file di archivio o compressi che potrebbero contenere malware verranno bloccati dalla scansione in accesso:</p> <ul style="list-style-type: none"> ■ Quando si apre un file estratto dal file di archivio, tale file viene sottoposto a scansione. ■ I file compressi tramite utilità di compressione dinamiche, quali PKLite, LZEXE e Diet, vengono sottoposti a scansione.
Scansione della memoria di sistema	Abilitare questa opzione per seguire automaticamente una scansione di background a cadenza oraria per rilevare malware nascosti nella memoria di sistema del computer (la memoria utilizzata dal sistema operativo).
Esegui scansione a priorità più bassa	In Windows Vista e superiore, eseguire la scansione personalizzata con priorità più bassa in modo tale da avere un impatto minimo sulle applicazioni per gli utenti.

4.3.6.4 Configurazione della disinfezione per una scansione personalizzata

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Per configurare la disinfezione per una scansione personalizzata:

1. Nella **Home** page, sotto **Antivirus e HIPS**, cliccare su **Scansioni**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nell'elenco **Scansioni disponibili**, selezionare la scansione che si desidera modificare e poi cliccare su **Modifica**.
3. Cliccare su **Configura scansione**.
4. Cliccare sulla scheda **Disinfezione**.
5. Per disinfettare automaticamente i file infetti, in **Virus/spyware**, selezionare la casella di spunta **Disinfetta automaticamente i file contenenti virus o spyware**.

6. Selezionare l'azione che Sophos Anti-Virus dovrà intraprendere contro gli oggetti infetti, nel caso la disinfezione automatica non sia stata abilitata o non riesca:

Opzione	Descrizione
Solo log	Sophos Anti-Virus si limita a registrare gli oggetti infetti nel log della scansione personalizzata. Consultare la sezione Visualizzazione del log per la scansione personalizzata a pagina 27. Si tratta di un'impostazione predefinita.
Cancella Sposta in	Utilizzate queste impostazioni soltanto su consiglio del supporto tecnico di Sophos. Utilizzare altrimenti il Quarantine Manager per disinfettare il computer dai virus e spyware rilevati da Sophos Anti-Virus . Consultare la sezione Gestione di virus e spyware in quarantena a pagina 37.

7. In **File sospetti**, selezionare l'azione che Sophos Anti-Virus intraprenderà al rilevare file contenenti codici utilizzati comunemente da malware:

Opzione	Descrizione
Solo log	Sophos Anti-Virus si limita a registrare gli oggetti infetti nel log della scansione. Si tratta di un'impostazione predefinita.
Cancella Sposta in	Utilizzate queste impostazioni soltanto su consiglio del supporto tecnico di Sophos. Utilizzare altrimenti il Quarantine Manager per disinfettare il computer dai virus e spyware rilevati da Sophos Anti-Virus . Consultare la sezione Gestione di file sospetti in quarantena a pagina 39

8. Per rimuovere i componenti conosciuti di adware e Potentially Unwanted Applications (PUA) dai computer di tutti gli utenti, in **Adware e PUA**, selezionare la casella di spunta **Disinfetta automaticamente adware e PUA**.

La rimozione non annulla le modifiche già apportate da adware o PUA.

- Per informazioni su come visionare nel sito web di Sophos gli effetti collaterali di adware o PUA, consultare la sezione [Informazioni sulla disinfezione](#) a pagina 43.
- Per informazioni su come disinfettare il computer da adware e PUA utilizzando il Quarantine Manager, consultare la sezione [Gestione di adware e PUA in quarantena](#) a pagina 38 .

4.3.6.5 Pianificazione di una scansione personalizzata

Se si appartiene al gruppo SophosAdministrator, è possibile pianificare una scansione personalizzata o visualizzare e modificare le scansioni pianificate create da altri utenti.

1. Nella **Home** page, sotto **Antivirus e HIPS**, cliccare su **Scansioni**.

Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.

2. Nell'elenco **Scansioni disponibili**, selezionare la scansione che si desidera modificare e poi cliccare su **Modifica**.
3. Cliccare su **Pianifica scansione**.
4. Nella finestra di dialogo **Pianifica scansione**, selezionare **Abilita operazione pianificata**.
Selezionare il giorno o i giorni nei quali la scansione dovrà essere eseguita.
Aggiungere l'orario (o gli orari) cliccando su **Aggiungi**.
Se necessario, rimuovere o modificare un orario selezionandolo e cliccando rispettivamente su **Rimuovi** o **Modifica**.
5. Digitare *nome utente e password*. Assicurarsi che il campo relativo alla password non sia vuoto.
La scansione pianificata viene eseguita con i diritti di accesso di quell'utente.

Nota: Se la scansione rileva componenti di una minaccia nella memoria, e non è stata impostata la scansione per la disinfezione automatica di virus/spyware, la scansione si blocca. Ciò avviene poiché procedere con la scansione potrebbe consentire la diffusione di questa minaccia. Occorre effettuare la disinfezione della minaccia, prima di poter eseguire nuovamente la scansione.

4.3.6.6 Esecuzione di una scansione personalizzata

Nota: non è possibile eseguire una scansione personalizzata pianificata manualmente. Le scansioni pianificate sono visualizzate nella lista **Scansioni disponibili** con un'icona a forma di orologio.

1. Nella **Home** page, sotto **Antivirus e HIPS**, cliccare su **Scansioni**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nell'elenco **Scansioni disponibili**, selezionare la scansione che si desidera eseguire e poi cliccare su **Avvia**.
Nella finestra di Sophos Endpoint Security and Control, viene visualizzata una finestra di dialogo che mostra l'avanzamento della scansione e il riquadro **Riepilogo delle attività**.

Nota: Se la scansione rileva componenti di una minaccia nella memoria, e non è stata impostata la scansione per la disinfezione automatica di virus/spyware, la scansione si blocca. Ciò avviene poiché procedere con la scansione potrebbe consentire la diffusione di questa minaccia. Occorre effettuare la disinfezione della minaccia, prima di poter eseguire nuovamente la scansione.

Se vengono individuate minacce o applicazioni controllate, cliccare su **Dettagli** e consultare *Gestione degli oggetti in quarantena*.

4.3.6.7 Rinomina di una scansione personalizzata

1. Nella **Home** page, sotto **Antivirus e HIPS**, cliccare su **Scansioni**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nell'elenco **Scansioni disponibili**, selezionare la scansione che si desidera modificare e poi cliccare su **Modifica**.
3. Nella casella **Nome scansione**, digitare il nuovo nome della scansione.

4.3.6.8 Visualizzazione del log per la scansione personalizzata

1. Nella **Home** page, sotto **Antivirus e HIPS**, cliccare su **Scansioni**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
 2. Nell'elenco **Scansioni disponibili**, cliccare su **Riepilogo** per la scansione personalizzata.
 3. Nella finestra di dialogo **Riepilogo**, cliccare sul link nella parte inferiore della finestra.
- Dalla pagina log, è possibile copiare il log negli appunti, oppure inviarlo per e-mail o stamparlo.
Per trovare un testo specifico all'interno del log, cliccare su **Trova** e inserire il testo desiderato.

4.3.6.9 Visualizzazione del riepilogo di una scansione personalizzata

1. Nella **Home** page, sotto **Antivirus e HIPS**, cliccare su **Scansioni**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nell'elenco **Scansioni disponibili**, cliccare su **Riepilogo** per la scansione personalizzata.

4.3.6.10 Cancellazione di una scansione personalizzata

1. Nella **Home** page, sotto **Antivirus e HIPS**, cliccare su **Scansioni**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nell'elenco **Scansioni disponibili**, selezionare la scansione che si desidera cancellare e poi cliccare su **Cancella**.

4.3.7 Esecuzione della scansione completa del computer

Per eseguire la scansione dell'intero sistema in uso nel computer, inclusi boot sector e memoria di sistema:

- ❖ Nella pagina **Home**, sotto **Antivirus e HIPS**, cliccare su **Scansione del computer**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.

Viene visualizzata una finestra di dialogo che mostra l'avanzamento della scansione e nella finestra **Sophos Endpoint Security and Control** compare il **Riepilogo delle attività**.

Nota: Se la scansione rileva componenti di una minaccia nella memoria, si interrompe. Ciò avviene poiché procedere con la scansione potrebbe consentire la diffusione di questa minaccia. Occorre effettuare la disinfezione della minaccia, prima di poter eseguire nuovamente la scansione.

Se vengono individuate minacce o applicazioni controllate, cliccare su **Dettagli** e consultare *Gestione degli oggetti in quarantena*.

4.4 Sophos Behavior Monitoring

4.4.1 Monitoraggio del comportamento

In quanto parte della scansione in accesso, Sophos Behavior Monitoring protegge i computer con sistema operativo Windows 2000 e successivo dalle minacce non identificate o del giorno zero, oltre che da comportamento sospetto.

Il rilevamento in fase di esecuzione può rilevare minacce che non possono essere identificate prima dell'esecuzione. Il monitoraggio del comportamento utilizza due metodi di rilevamento in fase di esecuzione per identificare eventuali minacce:

- Rilevamento di comportamento malevolo e sospetto
- Rilevamento di buffer overflow

Rilevamento di comportamento malevolo e sospetto

Il rilevamento di comportamento sospetto utilizza l'Host Intrusion Prevention System (HIPS) di Sophos per analizzare dinamicamente il comportamento di tutti i programmi in esecuzione sul computer, per rilevare e bloccare qualsiasi attività dall'aspetto malevolo. Per comportamento sospetto si intendono ad esempio le modifiche al registro che potrebbero consentire l'esecuzione automatica di un virus al riavvio del computer.

Il rilevamento di comportamento sospetto controlla tutti i processi di sistema alla ricerca di segni che indichino la presenza di malware attivo, quali scritture sospette nel registro o azioni di copiatura file. Può essere impostato in modo tale da avvertire l'amministratore e/o bloccare il processo.

Il rilevamento di comportamento malevolo coincide con l'analisi dinamica di tutti i programmi in esecuzione nel computer e ha lo scopo di rilevare e bloccare attività apparentemente malevoli.

Rilevamento di buffer overflow

Il rilevamento di buffer overflow è fondamentale nel trattamento delle minacce del giorno zero.

Analizza dinamicamente il comportamento dei programmi in esecuzione nel sistema per poter rilevare eventuali tentativi di sfruttare un processo in esecuzione tramite tecniche di buffer overflow. Intercetta attacchi che puntano a vulnerabilità della sicurezza nei software e applicazioni del sistema operativo.

4.4.2 Abilitazione del monitoraggio del comportamento

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Se parte del gruppo SophosAdministrator è possibile abilitare il monitoraggio del comportamento.

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Monitoraggio del comportamento** .

2. Nella finestra di dialogo **Configura monitoraggio del comportamento**, mettere la spunta nella casella **Abilita monitoraggio del comportamento**.

4.4.3 Blocco di comportamento malevolo

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Il rilevamento di comportamento malevolo coincide con l'analisi dinamica di tutti i programmi in esecuzione nel computer e ha lo scopo di rilevare e bloccare attività apparentemente malevoli.

Se membri del gruppo SophosAdministrator, è possibile modificare le impostazioni per il rilevamento e la segnalazione di comportamento malevolo:

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Monitoraggio del comportamento**.
2. Nella finestra di dialogo **Configura monitoraggio del comportamento**, mettere la spunta nella casella **Abilita monitoraggio del comportamento**.
3. Per allertare l'amministratore e bloccare episodi di comportamento malevolo, selezionare la casella di spunta **Rileva comportamento malevolo**.

4.4.4 Prevenzione di comportamento sospetto

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Il rilevamento di comportamento sospetto controlla tutti i processi di sistema alla ricerca di segni che indichino la presenza di malware attivo, quali scritture sospette nel registro o azioni di copiatura file. Può essere impostato in modo tale da avvertire l'amministratore e/o bloccare il processo.

Se membri del gruppo SophosAdministrator, è possibile modificare le impostazioni per il rilevamento e la segnalazione di comportamento sospetto:

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Monitoraggio del comportamento**.
2. Nella finestra di dialogo **Configura monitoraggio del comportamento**, mettere la spunta nella casella **Abilita monitoraggio del comportamento**.
3. Selezionare la casella di spunta **Rileva comportamento malevolo**.
4. Per allertare l'amministratore e bloccare eventuali processi sospetti, selezionare la casella **Rileva comportamento malevolo**.
5. Per allertare l'amministratore, ma non bloccare eventuali processi sospetti, selezionare la casella di spunta **Avvisa solo, non bloccare comportamento sospetto**.

Per avere protezione massima, si consiglia di abilitare il rilevamento di file sospetti. Per ulteriori informazioni, consultare i seguenti argomenti:

- [Configurazione della scansione in accesso](#) a pagina 8
- [Configurazione della scansione dal menu del tasto destro del mouse](#) a pagina 19
- [Configurazione di una scansione personalizzata](#) a pagina 22

4.4.5 Prevenzione di buffer overflow

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Il rilevamento di buffer overflow analizza dinamicamente il comportamento dei programmi in esecuzione nel sistema per poter rilevare eventuali tentativi di sfruttare un processo in esecuzione tramite tecniche di buffer overflow.

Se membri del gruppo SophosAdministrator, è possibile modificare le impostazioni per il rilevamento e la segnalazione di buffer overflow:

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Monitoraggio del comportamento**.
2. Nella finestra di dialogo **Configura monitoraggio del comportamento**, mettere la spunta nella casella **Abilita monitoraggio del comportamento**.
3. Per avvisare l'amministratore e bloccare il buffer overflow, selezionare la casella di spunta **Rileva buffer overflow**.
4. Per allertare l'amministratore, ma non bloccare episodi di buffer overflow, selezionare la casella di spunta **Avvisa solo, non bloccare**.

4.5 Sophos Live Protection

4.5.1 Sophos Live Protection

Sophos Live Protection decide se un file sospetto rappresenta una minaccia e, quando ciò accade, agisce immediatamente secondo quanto specificato nella configurazione disinfezione di Sophos Anti-Virus.

Sophos Live Protection migliora il rilevamento di nuovo malware, senza il rischio di rilevamenti indesiderati. Questo avviene mediante ricerca istantanea in base alle più aggiornate versioni di malware conosciute. Quando viene identificato un nuovo malware, Sophos è in grado di inviare aggiornamenti entro pochi secondi.

Sophos Live Protection utilizza le seguenti opzioni:

■ **Abilita Live Protection**

Se la scansione antivirus su un computer ha identificato un file come sospetto, ma non riesce poi a determinare se sia pulito o malevolo, in base ai file di identità delle minacce (IDE) memorizzati nel computer, alcuni dati del file (come il checksum e altri attributi) vengono inviati a Sophos per un'ulteriore analisi.

La verifica "in-the-cloud" esegue la ricerca istantanea di un file sospetto nel database di SophosLabs. Se il file viene identificato come pulito o malevolo, la decisione viene inviata al computer e lo stato del file viene automaticamente aggiornato.

■ **Invio automatico dei file campione a Sophos**

Se un file viene considerato sospetto, ma non può essere identificato con certezza come malevolo solo in base ai suoi dati, è possibile permettere la richiesta da parte di Sophos di

un campione del file. Se tale opzione è abilitata, e Sophos non detiene ancora un campione del file, il file verrà inviato automaticamente.

L'invio di file campione permette a Sophos di migliorare continuamente il rilevamento del malware senza il rischio di falsi positivi.

4.5.2 Attivazione e disattivazione delle opzioni di Sophos Live Protection

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Se si appartiene al gruppo SophosAdministrator, è possibile attivare o disattivare Sophos Live Protection:

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Sophos Live Protection**.
2. Nella finestra di dialogo **Sophos Live Protection**:
 - Per attivare o disattivare l'invio a Sophos di dati dei file, selezionare o deselezionare la casella di spunta **Abilita Live Protection**.
 - Per attivare o disattivare l'invio a Sophos di campioni di file, selezionare o deselezionare la casella di spunta **Invio automatico dei file campione a Sophos**.

Questa opzione è disponibile solamente se **Abilita Live Protection** è già stata selezionata.

Nota

Quando si invia il campione di un file a Sophos per la scansione in linea, insieme al campione vengono sempre inviati i dati del file.

4.5.3 Visualizzazione del log di Sophos Live Protection

I dati dei file inviati a Sophos per le scansioni in linea e gli aggiornamenti di stato dei file una volta completate le scansioni vengono registrati nel log della scansione del computer.

Se Sophos Live Protection è attiva, il log mostra:

- Il percorso di tutti i file, i cui dati sono stati inviati a Sophos.
- L'orario in cui tali dati sono stati inviati
- La causa dell'errore (se conosciuta) se l'invio dei dati non è riuscito.
- Lo stato attuale del file (per esempio, "virus/spyware" se il file è stato identificato come malevolo).

Per visualizzare il log della scansione:

- Nella pagina **Home**, sotto **Antivirus ed HIPS**, cliccare su **Visualizza log antivirus e HIPS**. Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.

Dalla pagina log, è possibile copiare il log negli appunti, oppure inviarlo per e-mail o stamparlo.

Per trovare un testo specifico all'interno del log, cliccare su **Trova** e inserire il testo desiderato.

4.6 Sophos Web Protection

4.6.1 Sophos Web Protection

Sophos Web Protection offre una protezione ancora più efficace contro le minacce web. Verifica gli URL dei siti web utilizzando il database online di Sophos alla ricerca di siti web infetti; nel caso di siti web noti per ospitare malware, l'accesso verrà bloccato.

I seguenti browser supportano la protezione web:

- Internet Explorer
- Firefox
- Google Chrome
- Safari
- Opera

Quando viene bloccato l'accesso a un sito web malevolo, viene registrato un evento nel log della scansione. Per informazioni sulla visualizzazione di eventi nel log della scansione, consultare la sezione [Visualizzazione del log della scansione](#) a pagina 48.

4.6.2 Sblocco dell'accesso a siti web malevoli

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Per sbloccare l'accesso a siti web malevoli:

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Web protection**.
2. Nell'elenco **Blocca l'accesso ai siti malevoli**, cliccare su **Disattivato**.
Per informazioni su come autorizzare un sito web classificato come malevolo, consultare la sezione [Autorizzazione all'utilizzo di un sito web](#) a pagina 34.
3. Dall'elenco **Scarica scansione**, cliccare su **Disattivato**, **Attivato** o **Come in accesso**.
Le impostazioni **Come in accesso** conserveranno quelle della scansione *in accesso*.

4.7 Sophos Application Control

4.7.1 Scansione per la ricerca di applicazioni controllate

Un'*applicazione controllata* è un'applicazione la cui esecuzione nel computer è impedita dai criteri di sicurezza aziendali.

La scansione alla ricerca di applicazioni controllate viene attivata o disattivata da una console di gestione come parte del criterio di controllo applicazioni e della scansione in accesso.

Per informazioni sulla scansione in accesso, consultare la sezione [Scansione in accesso e su richiesta](#) a pagina 8.

4.7.2 Disabilitazione della scansione alla ricerca di applicazioni controllate

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Se si attiva la scansione per la ricerca di applicazioni controllate, questa potrebbe impedire la disinstallazione di alcune applicazioni. Se si appartiene al gruppo SophosAdministrator, è possibile disabilitare temporaneamente la scansione alla ricerca di applicazioni controllate nel computer in questione.

Per disabilitare la scansione alla ricerca di applicazioni controllate:

1. Nel menu **Configura**, cliccare su **Controllo applicazioni**.
2. Deselezionare la casella **Abilita scansione in accesso**.

4.8 Autorizzazione all'utilizzo di oggetti

4.8.1 Autorizzazione all'utilizzo di adware e PUA

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Se si desidera eseguire adware o un'applicazione che Sophos Anti-Virus ha classificato come potenzialmente indesiderata, è possibile autorizzarla.

Per autorizzare l'utilizzo di adware e PUA:

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Autorizzazione**.
2. Nella scheda **Adware o PUA**, nell'elenco **Adware e PUA noti**, selezionare adware o PUA.
3. Cliccare su **Aggiungi**.

L'adware o PUA appare nell'elenco **Adware o PUA autorizzati**.

Nota: è anche possibile autorizzare adware e PUA nel gestore quarantena. Per informazioni su come svolgere questa operazione, consultare la sezione [Gestione di adware e PUA in quarantena](#) a pagina 38.

4.8.2 Blocco di adware e PUA autorizzati

Per evitare che adware e PUA attualmente autorizzati vengano eseguiti nel computer:

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Autorizzazione**.
2. Nella scheda **Adware o PUA**, nell'elenco **Adware o PUA autorizzati**, selezionare adware o PUA che si desidera bloccare.
3. Cliccare su **Rimuovi**.

4.8.3 Autorizzazione all'uso di oggetti sospetti

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Se si desidera autorizzare un oggetto che Sophos Anti-Virus ha classificato come sospetto, è possibile autorizzarlo nel modo seguente.

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Autorizzazione**.
2. Cliccare sulla scheda relativa al tipo di oggetto rilevato (per es. **Buffer overflow**).
3. Cliccare sull'elenco **Nota** e selezionare l'oggetto sospetto.
4. Cliccare su **Aggiungi**.

L'oggetto sospetto compare nell'elenco **Autorizzato**.

Nota: è anche possibile autorizzare oggetti sospetti nel Gestore quarantena. Per informazioni su come fare ciò, consultare le seguenti sezioni:

- [Gestione di file sospetti in quarantena](#) a pagina 39
- [Gestione di comportamento sospetto in quarantena](#) a pagina 40

4.8.4 Preautorizzazione di oggetti sospetti

Se si desidera autorizzare un oggetto che Sophos Endpoint Security and Control non ha ancora classificato come sospetto, è possibile preautorizzarlo.

Per preautorizzare un oggetto sospetto:

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Autorizzazione**.
2. Cliccare sulla scheda relativa al tipo di oggetto rilevato (per es. **Buffer overflow**).
3. Cliccare su **Nuova voce**.
4. Trovare l'oggetto sospetto e cliccarvi due volte.

L'oggetto sospetto compare nell'elenco **Autorizzato**.

4.8.5 Autorizzazione all'utilizzo di un sito web

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Se si desidera sbloccare un sito classificato come malevolo da Sophos, è possibile aggiungerlo all'elenco dei siti autorizzati. Gli URL di un sito web autorizzato non vengono verificati dal filtro web online di Sophos.



Attenzione: Autorizzare un sito web classificato come malevolo potrebbe esporre a minacce; assicurarsi che l'accesso al sito sia sicuro prima di autorizzarlo.

Per autorizzare l'utilizzo di un sito web:

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Configura > Autorizzazione**.
2. Cliccare sulla scheda **Siti web**.
3. Cliccare su **Aggiungi**.
4. Inserire il nome di dominio o l'indirizzo IP.

Il sito web compare nell'elenco dei **Siti web autorizzati**.

4.9 Gestione degli oggetti in quarantena

4.9.1 Gestore quarantena

Il Gestore quarantena consente di gestire gli oggetti individuati mediante la scansione e non eliminati automaticamente durante la stessa. Ciascun oggetto viene conservato qui per una delle ragioni seguenti.

- Non è stata scelta alcuna opzione di disinfezione (disinfezione, cancellazione, spostamento) per il tipo di scansione durante la quale è stato individuato l'oggetto.
- È stata scelta un'opzione di disinfezione per il tipo di scansione durante la quale è stato individuato l'oggetto, ma l'opzione non ha funzionato correttamente.
- L'oggetto ha un'infezione multipla e contiene ancora altre minacce.
- La minaccia è stata rilevata solo parzialmente. Per rilevarla in maniera completa, è necessaria una scansione completa del computer. Per maggiori informazioni su come effettuare tale operazione, consultare [Esecuzione della scansione completa del computer](#) a pagina 27.
- L'oggetto manifesta un comportamento sospetto.
- L'oggetto è un'applicazione controllata.

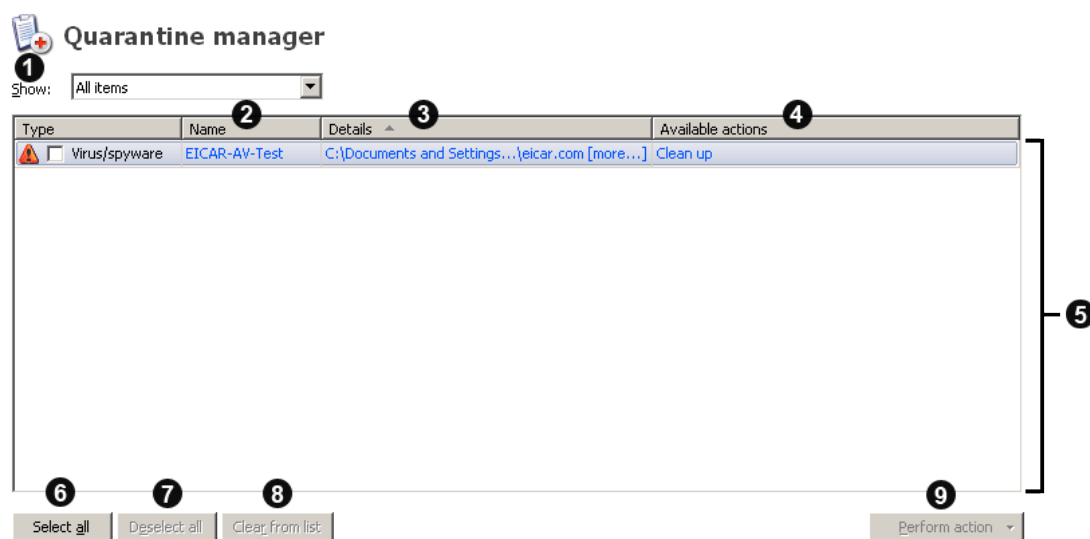
Nota: adware, PUA e infezioni multicomponente rilevate durante la scansione in accesso sono sempre elencate nel Gestore quarantena. La disinfezione automatica di adware, PUA e infezioni multicomponente non è disponibile per la scansione in accesso.

L'opzione di disinfezione potrebbe non aver funzionato correttamente a causa di diritti di accesso insufficienti. Se si dispone di diritti maggiori, è possibile utilizzare Gestore quarantena per gestire l'oggetto o gli oggetti.

Le minacce rilevate durante la scansione delle pagine web non sono elencate nel Gestore quarantena perché non vengono scaricate nel computer. Pertanto, in tali casi non è necessaria alcuna azione.

4.9.2 Layout del Gestore quarantena

Il Gestore quarantena elenca tutti gli oggetti rilevati durante la scansione rendendo possibile i relativi interventi da parte dell'utente. Gli elementi della finestra **Gestore quarantena** vengono illustrati qui di seguito.



1	Cliccare sull'elenco Mostra per filtrare i tipi di oggetti visualizzati.
2	L'identità dell'oggetto, completa di link alla sua analisi pubblicata sul sito web di Sophos.
3	Nome file e percorso dell'oggetto. Se l'oggetto risulta associato a un rootkit, viene visualizzato come Nascosto . Se accanto al nome del file appare il collegamento dettagli , significa che l'oggetto presenta un'infezione multicomponente. Cliccare sul link per visualizzare la lista degli altri componenti che formano l'infezione. Se alcuni componenti risultano associati a un rootkit, nella finestra di dialogo vengono indicati come nascosti.
4	L'azione da intraprendere su un determinato oggetto. Se l'oggetto non è nascosto, è possibile intraprendere tre tipi di azione: Disinfetta , Cancella e Sposta . Se si clicca su una delle azioni disponibili, tale azione verrà intrapresa non appena ricevuta conferma. I file nascosti possono essere solo disinfettati.
5	Elenco degli oggetti rilevati. Per ordinare gli oggetti è possibile cliccare sui titoli delle colonne.
6	Cliccare su Seleziona tutto per intraprendere la medesima azione su tutti gli oggetti. Per deselegionare un oggetto, deselegionare la relativa casella di spunta nella colonna Tipo .
7	Se in un primo tempo sono stati selezionati tutti gli oggetti, ma successivamente si desidera deselegionarli, cliccare su Deseleziona tutto . Per selezionare un oggetto, cliccare la relativa casella di spunta nella colonna Tipo .
8	Cliccare su Cancella dalla lista per eliminare gli oggetti selezionati dall'elenco, senza intraprendere alcuna azione su di essi. Comunque gli oggetti non vengono cancellati dal disco.

9	Cliccare su Esegui azione per visualizzare un elenco di azioni che è possibile intraprendere sugli oggetti selezionati.
----------	--------------------------------------------------------------------------------------------------------------------------------

4.9.3 Gestione di virus e spyware in quarantena

Nota: Il termine *virus* si riferisce a qualsiasi virus, worm o trojan o ad altro software malevolo.

1. Nella **Home** page, sotto **Antivirus e HIPS**, cliccare su **Gestisci elementi messi in quarantena**. Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nell'elenco **Mostra**, cliccare su **Virus/spyware**.

Nelle colonne sono visualizzate informazioni relative a ciascun oggetto.

Nome visualizza l'identità rilevata da Sophos Anti-Virus. Per ulteriori informazioni sul virus e spyware, cliccare sull'identità. Sophos Anti-Virus si connette quindi all'analisi del virus o spyware disponibile sul sito web di Sophos.

Dettagli visualizza il nome e la posizione dell'oggetto. Se l'oggetto è associato a un rootkit, viene visualizzato come "Nascosto". Se accanto al nome del file appare il collegamento **dettagli**, significa che l'oggetto presenta un'infezione multicomponente. Cliccare sul link per visualizzare la lista degli altri componenti che formano l'infezione. Se uno dei componenti è associato a un rootkit, la finestra di dialogo indica che alcuni componenti sono nascosti.

Azioni disponibili visualizza le azioni eseguibili sull'oggetto. A meno che l'oggetto non sia nascosto, sono disponibili tre azioni: Disinfetta, Cancella e Sposta, come descritto sotto. Cliccando su una delle azioni, l'azione viene eseguita sull'oggetto dopo la conferma. I file nascosti possono essere solo disinfettati.

Gestione degli oggetti infetti

Per gestire virus e spyware, utilizzare i pulsanti descritti sotto.

Seleziona tutto/Deseleziona tutto

Cliccare su questi pulsanti per selezionare oppure per deselegionare tutti gli oggetti. Ciò consente di eseguire la stessa azione su un gruppo di oggetti. Per selezionare o deselegionare un determinato oggetto, spuntare la casella alla sinistra del tipo di oggetto.

Cancella dalla lista

Cliccare su questa opzione per rimuovere dalla lista gli oggetti selezionati, se si è certi che non contengono virus o spyware. Comunque gli oggetti non vengono cancellati dal disco.

Esegui azione

Cliccare su questa opzione per visualizzare una lista di azioni eseguibili sugli oggetti selezionati.

- Cliccare su **Disinfetta** per rimuovere un virus o spyware dagli oggetti selezionati. La disinfezione dei documenti non annulla le modifiche che il virus può aver apportato al documento.

Nota: Per una rimozione completa dal computer di alcuni virus e spyware formati da diversi componenti, sarà necessario riavviare il computer. In questo caso viene data la

possibilità di riavviare il computer immediatamente o in un secondo tempo. Le operazioni conclusive di rimozione saranno eseguite dopo il riavvio del computer.

Nota: La disinfezione di alcuni virus provoca l'esecuzione di una scansione completa del sistema, la quale cerca di disinfettare *tutti* i virus. Ciò potrebbe richiedere molto tempo. L'azione disponibile cambia e diventa **Disinfezione** fino al completamento della scansione.

- Cliccare su **Cancella** per cancellare gli oggetti selezionati dal computer. Utilizzare questa funzione con cautela.
- Cliccare su **Sposta** per spostare gli oggetti selezionati in un'altra cartella. Gli oggetti vengono spostati nella cartella che è stata specificata durante l'impostazione della disinfezione. Spostando un file eseguibile si riducono le probabilità che venga eseguito. Utilizzare questa funzione con cautela.



Attenzione: talvolta, se si cancella o si sposta un file infetto, il computer può smettere di funzionare correttamente, perché non riesce a trovare il file. Inoltre, un file infetto può essere solo parte di un'infezione multipla, nel qual caso la sua cancellazione o il suo spostamento non comporterà la disinfezione del computer. In questo caso, rivolgersi al supporto tecnico di Sophos per ricevere assistenza nella gestione degli oggetti.

Per informazioni su come contattare il supporto tecnico, consultare la sezione [Supporto tecnico](#) a pagina 104.

Per configurare quali azioni poter svolgere, consultare la sezione [Configurazione dei diritti utente per il Gestore quarantena](#) a pagina 6.

4.9.4 Gestione di adware e PUA in quarantena

1. Nella **Home** page, sotto **Antivirus e HIPS**, cliccare su **Gestisci elementi messi in quarantena**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nell'elenco **Mostra**, cliccare su **Adware o PUA**.

Nelle colonne sono visualizzate informazioni relative a ciascun oggetto.

Nome visualizza l'identità rilevata da Sophos Anti-Virus. Per ulteriori informazioni sull'adware o PUA, cliccare sull'identità. Sophos Anti-Virus si connette quindi all'analisi dell'adware o PUA disponibile sul sito web di Sophos.

Dettagli visualizza il sottotipo di adware e PUA. Se l'oggetto è associato a un rootkit, viene visualizzato come "Nascosto". Se accanto al sottotipo appare il collegamento **dettagli**, significa che l'oggetto è un adware e PUA multicomponente. Cliccare sul link per visualizzare l'elenco degli altri componenti che formano l'adware o PUA. Se uno dei componenti è associato a un rootkit, la finestra di dialogo indica che alcuni componenti sono nascosti.

Azioni disponibili visualizza le azioni eseguibili sull'oggetto. Sono disponibili due azioni, autorizzazione e rimozione, come descritto sotto. Cliccando su una delle azioni, l'azione viene eseguita sull'oggetto dopo la conferma.

Gestione di adware e PUA

Per gestire adware e PUA, utilizzare i pulsanti descritti sotto.

Seleziona tutto/Deseleziona tutto

Cliccare su questi pulsanti per selezionare oppure per deselegionare tutti gli oggetti. Ciò consente di eseguire la stessa azione su un gruppo di oggetti. Per selezionare o deselegionare un determinato oggetto, spuntare la casella alla sinistra del tipo di oggetto.

Cancella dalla lista

Cliccare su questa opzione per rimuovere dalla lista gli oggetti selezionati, se sono affidabili. Comunque gli oggetti non vengono cancellati dal disco.

Esegui azione

Cliccare su questa opzione per visualizzare una lista di azioni eseguibili sugli oggetti selezionati.

- Cliccare su **Autorizza** per autorizzare nel computer gli oggetti selezionati, se sono affidabili. Tale opzione aggiunge gli oggetti alla lista degli adware e PUA autorizzati in modo che Sophos Anti-Virus non ne impedisca l'esecuzione nel computer.
- Cliccare su **Disinfetta** per rimuovere dal computer, per tutti gli utenti, tutti i componenti noti degli oggetti selezionati. Per rimuovere dal computer adware e PUA, è necessario che l'utente appartenga a entrambi i gruppi Windows Administrators e SophosAdministrator.

Nota: per una rimozione completa dal computer di alcuni adware e PUA formati da diversi componenti, sarà necessario riavviare il computer. In questo caso viene data la possibilità di scegliere di riavviare il computer immediatamente o in un secondo tempo. Le operazioni conclusive di rimozione saranno eseguite dopo il riavvio del computer.

Per configurare quali azioni poter svolgere, consultare la sezione [Configurazione dei diritti utente per il Gestore quarantena](#) a pagina 6

Per visualizzare la lista degli adware e PUA noti e autorizzati, cliccare su **Configura autorizzazione**.

4.9.5 Gestione di file sospetti in quarantena

Un *file sospetto* è un file che presenta una serie di caratteristiche comunemente, ma non esclusivamente, riscontrate in virus.

1. Nella **Home** page, sotto **Antivirus e HIPS**, cliccare su **Gestisci elementi messi in quarantena**. Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nell'elenco **Mostra**, cliccare su **File sospetti**.

Nelle colonne sono visualizzate informazioni relative a ciascun oggetto.

Nome visualizza l'identità rilevata da Sophos Anti-Virus. Per ulteriori informazioni sul file sospetto, cliccare sull'identità. Sophos Anti-Virus si connette quindi all'analisi del file sospetto disponibile sul sito web di Sophos.

Dettagli visualizza il nome e la posizione dell'oggetto. Se l'oggetto è associato a un rootkit, viene visualizzato come "Nascosto".

Azioni disponibili visualizza le azioni eseguibili sull'oggetto. A meno che l'oggetto non sia nascosto, sono disponibili tre azioni: Autorizza, Cancella e Sposta, come descritto sotto.

Cliccando su una delle azioni, l'azione viene eseguita sull'oggetto dopo la conferma. I file nascosti possono essere solo autorizzati.

Gestione dei file sospetti

Per gestire i file sospetti, utilizzare i pulsanti descritti sotto.

Seleziona tutto/Deseleziona tutto

Cliccare su questi pulsanti per selezionare oppure per deselegionare tutti gli oggetti. Ciò consente di eseguire la stessa azione su un gruppo di oggetti. Per selezionare o deselegionare un determinato oggetto, spuntare la casella alla sinistra del tipo di oggetto.

Cancella dalla lista

Cliccare su questa opzione per rimuovere dalla lista gli oggetti selezionati, se sono affidabili. Comunque gli oggetti non vengono cancellati dal disco.

Esegui azione

Cliccare su questa opzione per visualizzare una lista di azioni eseguibili sugli oggetti selezionati.

- Cliccare su **Autorizza** per autorizzare nel computer gli oggetti selezionati, se sono affidabili. Tale opzione aggiunge gli oggetti alla lista degli oggetti sospetti autorizzati in modo che Sophos Anti-Virus non impedisca l'accesso ad essi.
- Cliccare su **Cancella** per cancellare gli oggetti selezionati dal computer. Utilizzare questa funzione con cautela.
- Cliccare su **Sposta** per spostare gli oggetti selezionati in un'altra cartella. Gli oggetti vengono spostati nella cartella che è stata specificata durante l'impostazione della disinfezione. Spostando un file eseguibile si riducono le probabilità che venga eseguito. Utilizzare questa funzione con cautela.



Attenzione: talvolta, se si cancella o si sposta un file infetto, il computer può smettere di funzionare correttamente, perché non riesce a trovare il file.

Per configurare quali azioni poter svolgere, consultare la sezione [Configurazione dei diritti utente per il Gestore quarantena](#) a pagina 6

Per visualizzare la lista dei file sospetti autorizzati, cliccare su **Configura autorizzazione**.

4.9.6 Gestione di comportamento sospetto in quarantena

Il termine *Comportamento sospetto* indica un'attività apparentemente malevola.

1. Nella **Home** page, sotto **Antivirus e HIPS**, cliccare su **Gestisci elementi messi in quarantena**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nell'elenco **Mostra**, cliccare su **Comportamento sospetto**.

Nelle colonne sono visualizzate informazioni relative a ciascun oggetto.

Nome visualizza l'identità rilevata da Sophos Sophos Anti-Virus. Per ulteriori informazioni sul comportamento, cliccare sull'identità. Sophos Anti-Virus si connette quindi all'analisi del comportamento disponibile sul sito web di Sophos.

Dettagli visualizza il nome e la posizione dell'oggetto.

Azioni disponibili visualizza le azioni eseguibili sull'oggetto. Se è stato abilitato il blocco del comportamento sospetto è disponibile una sola azione: autorizzazione, come spiegato di seguito. Cliccando sull'azione, essa viene eseguita sull'oggetto dopo la conferma.

Gestione del comportamento sospetto

Per gestire il comportamento sospetto, utilizzare i pulsanti descritti sotto.

Seleziona tutto/Deseleziona tutto

Cliccare su questi pulsanti per selezionare oppure per deselezionare tutti gli oggetti. Ciò consente di eseguire la stessa azione su un gruppo di oggetti. Per selezionare o deselezionare un determinato oggetto, spuntare la casella alla sinistra del tipo di oggetto.

Cancella dalla lista

Cliccare su questa opzione per rimuovere dalla lista gli oggetti selezionati, se sono affidabili. Comunque gli oggetti non vengono cancellati dal disco.

Esegui azione

Cliccare su questa opzione per visualizzare una lista di azioni eseguibili sugli oggetti selezionati.

- Cliccare su **Autorizza** per autorizzare nel computer gli oggetti selezionati, se sono affidabili. Tale opzione aggiunge gli oggetti alla lista degli oggetti sospetti autorizzati in modo che Sophos Anti-Virus non ne impedisca l'esecuzione.

Per configurare quali azioni poter svolgere, consultare la sezione [Configurazione dei diritti utente per il Gestore quarantena](#) a pagina 6

Per visualizzare la lista dei comportamenti sospetti autorizzati, cliccare su **Configura autorizzazione**.

4.9.7 Gestione di applicazioni controllate in quarantena

Un'*applicazione controllata* è un'applicazione la cui esecuzione nel computer è impedita dai criteri di sicurezza aziendali.

1. Nella **Home** page, sotto **Antivirus e HIPS**, cliccare su **Gestisci elementi messi in quarantena**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nell'elenco **Mostra**, cliccare su **Applicazioni controllate**.

Nelle colonne sono visualizzate informazioni relative a ciascun oggetto.

Nome visualizza l'identità rilevata da Sophos Anti-Virus. Per ulteriori informazioni sull'applicazione controllata, cliccare sull'identità. Sophos Anti-Virus si connette quindi all'analisi dell'applicazione controllata disponibile sul sito web di Sophos.

Dettagli visualizza il sottotipo di applicazione controllata. Se accanto al sottotipo appare il collegamento **dettagli**, cliccarvi sopra per visualizzare l'elenco degli altri componenti che formano l'applicazione controllata.

Azioni disponibili visualizza le azioni eseguibili sull'oggetto. Tuttavia, non è disponibile alcuna azione per le applicazioni controllate a parte la cancellazione dell'oggetto dall'elenco, come descritto sotto.

Gestione delle applicazioni controllate

Per gestire le applicazioni controllate, utilizzare i pulsanti descritti sotto.

Seleziona tutto/Deseleziona tutto

Cliccare su questi pulsanti per selezionare oppure per deselezionare tutti gli oggetti. Ciò consente di eseguire la stessa azione su un gruppo di oggetti. Per selezionare o deselezionare un determinato oggetto, spuntare la casella alla sinistra del tipo di oggetto.

Cancella dalla lista

Cliccare su questa opzione per rimuovere gli oggetti selezionati dalla lista. Comunque gli oggetti non vengono cancellati dal disco. È necessario che le applicazioni controllate vengano autorizzate dalla console centrale prima di poterle utilizzare.

4.10 Disinfezione

4.10.1 Disinfezione

La disinfezione elimina le minacce presenti nel computer tramite una delle seguenti azioni:

- Rimuove virus/spyware dal settore di avvio del floppy disk, da documenti, programmi e qualsiasi altro oggetto sottoposto a scansione
- Sposta o cancella il file sospetto
- Cancella adware o PUA

Quando Sophos Anti-Virus esegue la disinfezione automatica degli oggetti contenenti virus/spyware, procederà alla cancellazione di tutto il malware puro, ma tenterà di disinfettare gli oggetti contaminati. I file sottoposti a disinfezione risultano danneggiati permanentemente, dal momento che la scansione antivirus non può sapere cosa contenessero i file contaminati prima di essere colpiti da infezione.

Disinfezione dei documenti

La disinfezione dei documenti non annulla gli effetti collaterali dovuti a virus/spyware nel documento. Consultare la sezione [Informazioni sulla disinfezione](#) a pagina 43 per sapere come visualizzare, sul sito web di Sophos, i dettagli sugli effetti secondari dei virus/spyware.

Disinfezione dei programmi

La disinfezione dei programmi deve essere usata soltanto come misura temporanea. È poi necessario sostituire i programmi disinfettati a partire dai dischi originali o da una copia di backup pulita.

Disinfezione delle minacce web

La disinfezione non è necessaria per le minacce rilevate tramite la scansione della pagina web perché non vengono scaricate nel computer.

Note

- La disinfezione non annulla le azioni eventualmente già compiute dalla minaccia.
- Tutte le azioni eseguite da Sophos Anti-Virus sugli oggetti infetti vengono registrate nel log del computer o nel log della scansione personalizzata. Consultare la sezione [Visualizzazione del log della scansione](#) a pagina 48 o [Visualizzazione del log della scansione personalizzata](#) a pagina 27.
- Per rimuovere completamente alcune infezioni multicomponente, sarà necessario riavviare il computer. In questo caso viene data la possibilità di scegliere di riavviare il computer immediatamente o in un secondo tempo. Le operazioni conclusive di rimozione saranno eseguite dopo il riavvio del computer.

4.10.2 Informazioni sulla disinfezione

Quando nel computer viene rilevata una minaccia, è importante controllarne l'analisi sul sito web di Sophos per avere informazioni e consigli sulla disinfezione. Far ciò da:

- Allarme sul desktop (scansione in accesso)
- Finestra di dialogo che mostra l'avanzamento della scansione (scansione personalizzata e scansione dal menu del tasto destro del mouse)
- Gestore quarantena (tutti i tipi di scansione)

Informazioni tramite l'allarme sul desktop

Se nel computer è abilitata la scansione in accesso, Sophos Anti-Virus visualizza un allarme sul desktop ogni volta che rileva una minaccia.

Nella finestra di messaggio, cliccare sul nome della minaccia sulla quale si desidera ottenere informazioni. Sophos Anti-Virus si collega all'analisi della minaccia sul sito web di Sophos.

Informazioni tramite la finestra di avanzamento della scansione

Per la scansione personalizzata o la scansione dal menu del tasto destro del mouse, nel log visualizzato nella finestra di avanzamento della scansione (o nella finestra di riepilogo della scansione, visualizzata al termine della scansione), cliccare sul nome della minaccia sulla quale si desidera ottenere informazioni.

Sophos Anti-Virus si collega all'analisi della minaccia sul sito web di Sophos.

Informazioni tramite Gestore quarantena

1. Nella **Home** page, sotto **Antivirus e HIPS**, cliccare su **Gestisci elementi messi in quarantena**. Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nella colonna **Nome**, cliccare sul nome della minaccia sulla quale si desidera ottenere informazioni.

Sophos Anti-Virus si collega all'analisi della minaccia sul sito web di Sophos.

4.11 Configurazione degli allarmi

4.11.1 Configurazione della messaggistica desktop relativa all'antivirus

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Per consentire a Sophos Anti-Virus di visualizzare i messaggi sul desktop quando viene rilevata una minaccia, procedere come segue. Ciò vale soltanto per la scansione in accesso.

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Allarmi > Messaggistica** .
2. Nella finestra di dialogo **Messaggistica**, cliccare sulla scheda **Messaggistica desktop**. Impostare le opzioni come descritto di seguito.

Abilita messaggistica desktop

Selezionare questa opzione per consentire a Sophos Anti-Virus di visualizzare i messaggi sul desktop quando viene rilevata una minaccia.

Messaggi da inviare

Selezionare gli eventi per i quali si desidera che Sophos Anti-Virus visualizzi i messaggi sul desktop.

Messaggio definito dall'utente

In questa casella di testo è possibile digitare un messaggio che sarà aggiunto alla fine del messaggio standard.

4.11.2 Configurazione di allarmi antivirus tramite e-mail

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Per consentire a Sophos Anti-Virus di inviare degli allarmi e-mail quando viene rilevata una minaccia o quando si verifica un errore, procedere nel modo seguente. Ciò vale per la scansione in accesso, per la scansione su richiesta e per la scansione dal menu del tasto destro del mouse.

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Allarmi > Messaggistica** .

2. Nella finestra di dialogo **Messaggistica**, cliccare sulla scheda **Allarmi e-mail**. Impostare le opzioni come descritto di seguito.

Abilita allarmi e-mail

Selezionare questa opzione per consentire a Sophos Anti-Virus di inviare degli allarmi e-mail.

Messaggi da inviare

Selezionare gli eventi per i quali si desidera che Sophos Anti-Virus invii degli allarmi e-mail. Gli **errori di scansione** sono gli errori che si verificano quando a Sophos Anti-Virus viene negato l'accesso a un oggetto che tenta di esaminare.

Sophos Anti-Virus non invia allarmi e-mail relativi alla minacce rilevate dalla scansione delle pagine web perché tali minacce non vengono scaricate nel computer. Pertanto, in tali casi non è necessaria alcuna azione.

Destinatari

Cliccare su **Aggiungi** o **Rimuovi** per aggiungere o rimuovere, rispettivamente, gli indirizzi e-mail ai quali devono essere inviati gli allarmi e-mail. Cliccare su **Modifica** per modificare un indirizzo e-mail che è stato aggiunto.

Configura SMTP

Cliccare su questa opzione per modificare le impostazioni del server SMTP e la lingua degli allarmi e-mail. (v. la tabella di seguito).

Configurazione delle impostazioni di SMTP	
Server SMTP	Nella casella di testo, digitare il nome host o l'indirizzo IP del server SMTP. Cliccare su Prova per verificare che sia stata stabilita la connessione con il server SMTP (<i>non</i> viene inviata un'e-mail di prova).
Indirizzo SMTP "mittente"	Nella casella di testo, digitare un indirizzo e-mail al quale possono essere inviati bounce e messaggi di mancato recapito.
Indirizzo SMTP "rispondi a"	Poiché gli allarmi e-mail vengono inviati automaticamente dal sistema, è possibile digitare nella casella di testo un indirizzo e-mail al quale inviare gli allarmi stessi.
Language	Cliccare sulla freccia del menu a discesa e selezionare la lingua nella quale devono essere inviati gli allarmi e-mail.

4.11.3 Configurazione della messaggistica SNMP relativa all'antivirus

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Per consentire a Sophos Anti-Virus di inviare dei messaggi SNMP quando viene rilevata una minaccia o si verifica un errore, procedere nel modo seguente. Ciò vale per la scansione in accesso, per la scansione su richiesta e per la scansione dal menu del tasto destro del mouse.

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Allarmi > Messaggistica**.
2. Nella finestra di dialogo **Messaggistica**, cliccare sulla scheda **Messaggistica SNMP**. Impostare le opzioni come descritto di seguito.

Abilita messaggistica SNMP

Selezionare questa opzione per consentire a Sophos Anti-Virus di inviare dei messaggi SNMP.

Messaggi da inviare

Selezionare gli eventi per i quali si desidera che Sophos Anti-Virus invii messaggi SNMP. Gli **errori di scansione** sono gli errori che si verificano quando a Sophos Anti-Virus viene negato l'accesso a un oggetto che tenta di esaminare.

Sophos Anti-Virus non invia messaggi SNMP relativi alla minacce rilevate dalla scansione delle pagine web perché tali minacce non vengono scaricate nel computer. Pertanto, in tali casi non è necessaria alcuna azione.

Destinazione trap SNMP

Nella casella di testo, digitare l'indirizzo IP o il nome del computer al quale vengono inviati gli allarmi.

Nome comunità SNMP

Nella casella di testo, digitare il nome della comunità SNMP.

Prova

Cliccare su questo pulsante per inviare un messaggio SNMP di prova alla destinazione del trap SNMP che è stata specificata.

4.11.4 Configurazione del log eventi dell'antivirus

Per consentire a Sophos Anti-Virus di aggiungere gli allarmi al log degli eventi di Windows 2000 o successivo quando viene rilevata una minaccia o si verifica un errore, procedere nel modo seguente. Ciò vale per la scansione in accesso, per la scansione su richiesta e per la scansione dal menu del tasto destro del mouse.

1. Cliccare su **Home > Antivirus e HIPS > Configura antivirus e HIPS > Allarmi > Messaggistica**.

2. Nella finestra di dialogo **Messaggistica**, cliccare sulla scheda **Log eventi**. Impostare le opzioni come descritto di seguito.

Abilita log eventi

Selezionare questa opzione per consentire a Sophos Anti-Virus di inviare i messaggi al log degli eventi di Windows.

Messaggi da inviare

Selezionare gli eventi per i quali si desidera che Sophos Anti-Virus invii i messaggi. Gli **errori di scansione** sono gli errori che si verificano quando a Sophos Anti-Virus viene negato l'accesso a un oggetto che tenta di esaminare.

Sophos Anti-Virus non invia messaggi relativi alla minacce rilevate dalla scansione delle pagine web perché tali minacce non vengono scaricate nel computer. Pertanto, in tali casi non è necessaria alcuna azione.

4.12 Log scansione

4.12.1 Configurazione del log della scansione

Il log della scansione del computer si trova nei seguenti percorsi:

Windows Vista, Windows 7	C:\ProgramData\Sophos\Sophos Anti-Virus\logs\SAV.txt
Altre piattaforme Windows	C:\Documents and Settings\All Users\Dati applicazioni\Sophos\Sophos Anti-Virus\logs\SAV.txt

1. Cliccare su **Home > Antivirus e HIPS > Visualizza log antivirus e HIPS > Configura log**.
2. Nella finestra di dialogo **Configura log del computer**, impostare le opzioni come descritto sotto.

Livello di log

Per evitare che venga creato il log, cliccare su **Nessuno**. Per registrare le informazioni di riepilogo, i messaggi di errore e così via, cliccare su **Normale**. Per registrare la maggior parte delle informazioni, inclusi i file esaminati, le fasi principali di una scansione e così via, cliccare su **Dettagliato**.

Archiviazione del log

Affinché il file di log venga archiviato ogni mese, selezionare **Consenti archiviazione**. I file di archivio sono memorizzati nella stessa cartella del file di log. Selezionare il **Numero dei file di archivio** da memorizzare prima di cancellare il meno recente. Selezionare **Comprimi log** per ridurre le dimensioni del file di log.

4.12.2 Visualizzazione del log della scansione

- ❖ Nella pagina **Home**, sotto **Antivirus ed HIPS**, cliccare su **Visualizza log antivirus e HIPS**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.

Dalla pagina log, è possibile copiare il log negli appunti, oppure inviarlo per e-mail o stamparlo.
Per trovare un testo specifico all'interno del log, cliccare su **Trova** e inserire il testo desiderato.

5 Sophos Device Control

5.1 Controllo dispositivi nel computer

Se non viene utilizzata la console di gestione per amministrare Sophos Endpoint Security and Control nel computer, la funzionalità del controllo dispositivi *non* sarà inclusa.

Il controllo dispositivi viene abilitato o disabilitato dalla console di gestione. Se il controllo dispositivi è abilitato, impedirà la connessione di un dispositivo al computer anche se eseguito per motivi di manutenzione o per la risoluzione di alcuni problemi. Se questo è il caso, in tale computer è possibile disabilitare temporaneamente il controllo dispositivi. Per informazioni, consultare la sezione [Disabilitazione temporanea del controllo dispositivi](#) a pagina 49.

5.2 Tipi di dispositivo controllabili

Il controllo dispositivi blocca o consente tre tipi di dispositivi presenti nel computer: *memorizzazione, rete e short range*.

Memorizzazione

- Dispositivo di memoria rimovibile (per esempio unità flash USB, lettori di schede per PC, unità hard disk esterne)
- Unità disco ottico (unità CD-ROM/DVD/Blu-ray)
- Unità floppy disk
- Dispositivi di memorizzazione rimovibili sicuri (per esempio unità flash USB a cifratura basata su hardware)

Rete

- Modem
- Wireless (interfaccia Wi-Fi, 802.11 standard)

Il criterio di controllo dispositivi per questo computer potrebbe essere nella modalità **Block bridged**, che disattiva le schede di rete wireless o modem quando il computer è collegato a una rete fisica (di solito, attraverso una connessione Ethernet). Quando il computer è scollegato dalla rete fisica, le schede di rete wireless o modem vengono riabilitati direttamente.

Short range

- Interfacce Bluetooth
- Infrarossi (Interfaccia infrarossi IrDA)

5.3 Disabilitazione temporanea del controllo dispositivi

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Se si appartiene al gruppo Sophos Administrator e si desidera connettere un dispositivo al computer per motivi di manutenzione o per la risoluzione di alcuni problemi (per es. per installare un software da CD), è possibile disattivare temporaneamente il controllo dei dispositivi.

Per disabilitare il controllo dei dispositivi nel computer:

1. Nel menu **Configura**, cliccare su **Controllo dispositivi**.
2. Deselezionare la casella di spunta **Abilita Sophos Device Control**.

5.4 Configurazione del log del controllo dispositivi

1. Nel menu **Configura**, cliccare su **Controllo dispositivi**.
2. Sotto **Livello di log**, selezionare una delle opzioni:
 - Cliccare su **Nessuno** per impedire che venga creato il log.
 - Per registrare le informazioni di riepilogo, i messaggi di errore e così via, cliccare su **Normale**.
 - Cliccare su **Dettagliato** per ottenere informazioni relative a molte più attività del normale. Utilizzare questa impostazione solo quando è richiesto un log dettagliato per la risoluzione dei problemi, dal momento che le dimensioni del log cresceranno rapidamente.
3. Sotto **Archiviazione log**, seguire le istruzioni a schermo.

5.5 Visualizzazione del log del controllo dispositivi

- ❖ Nella **Home page**, sotto **Controllo dispositivi**, cliccare su **Visualizzare log controllo dispositivi**.

Per informazioni relative alla **Home page**, consultare la sezione [Home page](#) a pagina 4.

Dalla pagina log, è possibile copiare il log negli appunti, oppure inviarlo per e-mail o stamparlo.

Per trovare un testo specifico all'interno del log, cliccare su **Trova** e inserire il testo desiderato.

6 Sophos Data Control

6.1 Controllo dati nel computer

Se non viene utilizzata la console di gestione per amministrare Sophos Endpoint Security and Control nel computer, la funzionalità del controllo dati *non* sarà inclusa.

Il controllo dati viene abilitato o disabilitato da un criterio rilasciato da una console di gestione. Tuttavia, se si appartiene al gruppo SophosAdministrator, è possibile disabilitare temporaneamente il controllo dati nel computer per motivi di manutenzione o per la risoluzione di alcuni problemi: Per informazioni, consultare la sezione [Disabilitazione temporanea del controllo dati](#) a pagina 51.

6.2 Disabilitazione temporanea del controllo dati

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Se si appartiene al gruppo SophosAdministrator, è possibile disabilitare temporaneamente il controllo dati nel computer per motivi di manutenzione o per la risoluzione di alcuni problemi.

1. Nel menu **Configura**, cliccare su **Controllo dati**.
2. Deselezionare la casella di spunta **Abilita Sophos Data Control**.

6.3 Aggiunta di un file a un dispositivo di memorizzazione

Se in questo computer è abilitato il controllo dati, il criterio di controllo dati potrebbe bloccare qualsiasi tentativo di aggiunta di un file a un dispositivo di memorizzazione monitorato utilizzando i seguenti metodi:

- Salvataggio di dati all'interno di un programma
- Utilizzo del comando DOS copia
- Creazione di un nuovo file nel dispositivo che esegue Windows Explorer

Se si vede un allarme desktop in merito, è opportuno salvare il file sul disco rigido o su un'unità di rete e quindi utilizzare Esplora risorse per copiarlo sul dispositivo di memorizzazione.

6.4 Configurazione del log del controllo dati

1. Nel menu **Configura**, cliccare su **Controllo dati**.

2. Sotto **Livello di log**, selezionare una delle opzioni:
 - Cliccare su **Nessuno** per impedire che venga creato il log.
 - Per registrare le informazioni di riepilogo, i messaggi di errore e così via, cliccare su **Normale**.
 - Cliccare su **Dettagliato** per ottenere informazioni relative a molte più attività del normale. Utilizzare questa impostazione solo se si devono testare nuove regole del controllo dati, dal momento che le dimensioni del log cresceranno rapidamente.
3. Sotto **Archiviazione log**, seguire le istruzioni a schermo.

6.5 Visualizzazione del log del controllo dati

- ❖ Nella **Home page**, sotto **Controllo dati**, cliccare su **Visualizza log controllo dati**.
Per informazioni relative alla **Home page**, consultare la sezione [Home page](#) a pagina 4.

Dalla pagina log, è possibile copiare il log negli appunti, oppure inviarlo per e-mail o stamparlo.

Per trovare un testo specifico all'interno del log, cliccare su **Trova** e inserire il testo desiderato.

7 Sophos Client Firewall

7.1 Introduzione al firewall

Quando il firewall viene installato per la prima volta, può essere necessario configurarlo. Se sia necessario farlo o meno dipende dal modo in cui è stato installato. Sono disponibili due tipi di installazione:

- Installato in un computer in rete e gestito da una console di gestione
- Installato in un computer autonomo e gestito dal computer

Firewall gestito da una console di gestione

Se il firewall è installato e gestito da una console di gestione, consente o blocca applicazioni e traffico secondo le regole impostate dal criterio.

A meno che il criterio non abbia posto il firewall in modalità interattiva (v. sotto), l'utente non riceverà alcun messaggio e non dovrà configurare il firewall in alcun modo.

Firewall gestito dal computer

Se il firewall è gestito nel computer, si consiglia di cominciare creando regole che consentano l'accesso alla rete per applicazioni e servizi comuni, quali browser web e client di posta elettronica.

Per informazioni sulla creazione di regole, consultare la sezione [Configurazione del firewall](#) a pagina 53.

Inizialmente il firewall sarà in modalità interattiva (v. sotto). Lasciarlo in tale modalità per un periodo di tempo sufficiente a consentire o bloccare altri servizi e applicazioni in uso.

Una volta configurato il firewall e assicuratisi che riconosca le applicazioni comunemente utilizzate, si consiglia di passare a una delle modalità non interattive.

Per informazioni, consultare la sezione [Passaggio alla modalità non interattiva](#) a pagina 61.

Modalità interattiva

Quando in modalità interattiva, il firewall chiede di consentire o bloccare le applicazioni e il traffico per cui non sono state create regole.

Per informazioni su come gestire messaggi dal firewall, consultare la sezione [Modalità interattiva](#) a pagina 60.

7.2 Configurazione del firewall

7.2.1 Configurazione del firewall

È possibile configurare il firewall in molti modi diversi e poi abilitarlo. Tuttavia, se su questo computer viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control, essa potrebbe ignorare le modifiche qui apportate.

Alcune funzioni comuni sono elencate di seguito:

- [Abilitazione della modalità interattiva](#) a pagina 60
- [Filtraggio dei messaggi ICMP](#) a pagina 59
- [Autorizzazione di tutto il traffico su una LAN](#) a pagina 55
- [Autorizzazione del download del FTP](#) a pagina 55
- [Creazione di una regola globale](#) a pagina 67
- [Autorizzazione di un'applicazione](#) a pagina 57
- [Autorizzazione dell'avvio di processi nascosti](#) a pagina 71
- [Autorizzazione dell'utilizzo di raw socket da parte di applicazioni](#) a pagina 72
- [Utilizzo di checksum per l'autenticazione di applicazioni](#) a pagina 72

7.2.2 Disabilitazione temporanea del firewall

Se si appartiene al gruppo SophosAdministrator, può presentarsi la necessità di disabilitare temporaneamente il firewall per motivi di manutenzione o per la risoluzione di alcuni problemi e successivamente di riabilitarlo.

Sophos Endpoint Security and Control conserva le impostazioni scelte in questa pagina, anche dopo il riavvio del computer. Se si disabilita il firewall, il computer risulta non protetto finché la scansione in accesso non venga riabilitata.

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, selezionare la casella di spunta **Consenti tutto il traffico** di fianco al percorso primario o secondario.

7.2.3 Autorizzazione di e-mail

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Applicazioni**.
4. Cliccare su **Aggiungi**, trovare l'applicazione di posta elettronica e cliccarvi due volte.

L'applicazione di posta elettronica viene autorizzata in quanto applicazione attendibile.

Alle applicazioni attendibili viene concesso accesso alla rete pieno e incondizionato, oltre che accesso a Internet. Per una maggiore sicurezza, è possibile applicare le regole predefinite fornite da Sophos:

1. Nell'elenco delle applicazioni consentite, cliccare sull'applicazione di posta elettronica.

2. Cliccare su **Applicazione personalizzata > Aggiungi regole da quelle predefinite > Client di posta elettronica** .

7.2.4 Autorizzazione all'utilizzo di un browser web

Nota: se si consente l'utilizzo di un browser web, si consente al tempo stesso l'accesso FTP.

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Applicazioni**.
4. Cliccare su **Aggiungi**, trovare l'applicazione del browser web e cliccarvi due volte.

L'applicazione del browser web viene autorizzata in quanto applicazione attendibile.

Alle applicazioni attendibili viene concesso accesso alla rete pieno e incondizionato, oltre che accesso a Internet. Per una maggiore sicurezza, è possibile applicare le regole predefinite fornite da Sophos:

1. Nell'elenco delle applicazioni consentite, cliccare sull'applicazione del browser web.
2. Cliccare su **Personalizza > Aggiungi regole da quelle predefinite > Browser** .

7.2.5 Autorizzazione del download del FTP

Nota: se è stato concesso l'utilizzo di un browser web che può accedere ai server FTP, non è necessario autorizzare anche i download del FTP.

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Applicazioni**.
4. Cliccare su **Aggiungi**, trovare l'applicazione del FTP e cliccarvi due volte.

L'applicazione del FTP viene autorizzata in quanto applicazione attendibile.

Alle applicazioni attendibili viene concesso accesso alla rete pieno e incondizionato, oltre che accesso a Internet. Per una maggiore sicurezza, è possibile applicare le regole predefinite fornite da Sophos:

1. Nell'elenco delle applicazioni consentite, cliccare sull'applicazione del FTP.
2. Cliccare su **Applicazione personalizzata > Aggiungi regole da quelle predefinite > Client FTP** .

7.2.6 Autorizzazione di tutto il traffico su una LAN

Per consentire tutto il traffico tra computer su una LAN (Area di Rete Locale):

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.

2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Nella scheda **LAN**, svolgere una delle seguenti operazioni:
 - Cliccare su **Rileva** per rilevare la LAN in cui si trova il computer ed aggiungerla all'elenco di indirizzi di rete.
 - Cliccare su **Aggiungi**. Nella finestra di dialogo **Seleziona indirizzo**, selezionare **Formato indirizzo**, digitare il nome di dominio o l'indirizzo IP e poi cliccare su **Aggiungi**.

Nota: Se viene selezionata **Rete locale (rilevata automaticamente)**, non c'è bisogno di digitare altro. Per informazioni sul rilevamento di una sottorete, consultare la sezione [Rilevamento della rete locale](#) a pagina 65.
4. Cliccare su **OK** per chiudere la finestra di dialogo **Seleziona indirizzo**.
5. Nell'elenco **Impostazioni LAN**, spuntare la casella **Attendibile** per una rete.

Nota

- Se si consente tutto il traffico tra computer su una LAN, si consente anche la condivisione file e stampanti su di essa.

7.2.7 Autorizzazione di tutte le condivisioni file e stampanti su una LAN

Nota: Se è già stato consentito tutto il traffico fra computer su una LAN (rete di area locale), non c'è bisogno di permettere anche la condivisione di file e di stampanti.

Per autorizzare tutte le condivisioni file e stampanti su una LAN:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Nella scheda **LAN**, svolgere una delle seguenti operazioni:
 - Cliccare su **Rileva** per rilevare la LAN in cui si trova il computer ed aggiungerla all'elenco di indirizzi di rete.
 - Cliccare su **Aggiungi**. Nella finestra di dialogo **Seleziona indirizzo**, selezionare **Formato indirizzo**, digitare il nome di dominio o l'indirizzo IP e poi cliccare su **Aggiungi**.

Nota: Se viene selezionata **Rete locale (rilevata automaticamente)**, non c'è bisogno di digitare altro. Per informazioni sul rilevamento di una sottorete, consultare la sezione [Rilevamento della rete locale](#) a pagina 65.
4. Cliccare su **OK** per chiudere la finestra di dialogo **Seleziona indirizzo**.
5. Nell'elenco delle **Impostazioni LAN**, selezionare la casella di spunta **NetBIOS** per consentire a una LAN la condivisione file e stampanti.

Per informazioni su come bloccare o consentire la condivisione di file e stampanti su LAN diverse da quelle contenute nella lista **Impostazioni LAN**, consultare le seguenti sezioni:

- [Blocco di condivisioni file e stampanti indesiderate](#) a pagina 57
- [Autorizzazione del controllo flessibile di condivisione file e stampanti](#) a pagina 57

Per informazione su come consentire tutto il traffico su una LAN, consultare la sezione [Autorizzazione di tutto il traffico su una LAN](#) a pagina 55.

7.2.8 Autorizzazione del controllo flessibile di condivisione file e stampanti

Se si desidera un controllo più flessibile della condivisione file e stampanti sulla propria rete (ad esempio, traffico NetBIOS unidirezionale), è sufficiente fare come segue:

1. Autorizzare la condivisione file e stampanti in LAN (reti di area locali) diverse da quelle presenti nell'elenco **Impostazioni LAN**. Ciò consente il traffico NetBIOS sulle LAN sottoposte alle regole del firewall.
2. Creare regole con elevata priorità che consentano la comunicazione a/da host tramite gli adeguati protocolli e porte NetBIOS. Si consiglia di creare delle regole che blocchino esplicitamente tutto il traffico di condivisione file e stampanti indesiderato, piuttosto che lasciarlo gestire dalla regola predefinita.

Per autorizzare la condivisione file e stampanti in LAN diverse da quelle presenti nell'elenco **Impostazioni LAN**:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Nella scheda **LAN**, deselezionare la casella **Blocca condivisione file e stampanti per altre reti**.

7.2.9 Blocco di condivisioni file e stampanti indesiderate

Per bloccare la condivisione di file e stampanti su reti diverse da quelle specificate nell'elenco **Impostazioni LAN** sulla scheda **LAN**:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Nella scheda **LAN**, deselezionare la casella **Blocca condivisione file e stampanti per altre reti**.

7.2.10 Autorizzazione di un'applicazione

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Applicazioni**.
4. Cliccare su **Aggiungi**, trovare l'applicazione e cliccarvi due volte.

L'applicazione viene consentita in quanto attendibile.

Alle applicazioni attendibili viene concesso accesso alla rete pieno e incondizionato, oltre che accesso a Internet. per un maggior livello di sicurezza, è possibile applicare una o più *regole dell'applicazione* per specificare le condizioni in cui un'applicazione può essere eseguita.

- [Creazione di una regola dell'applicazione](#) a pagina 70
- [Applicazione delle regole delle applicazioni predefinite](#) a pagina 69

7.2.11 Blocco di un'applicazione

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Applicazioni**.
4. Se l'applicazione non è inclusa nell'elenco, cliccare su **Aggiungi**, trovare l'applicazione e cliccarvi due volte.
5. Selezionare l'applicazione nell'elenco e cliccare su **Blocca**.

7.2.12 Attivazione e disattivazione del blocco di processi modificati

Il malware potrebbe tentare di aggirare il firewall modificando un processo in memoria già iniziato da un programma attendibile, e utilizzare quindi il processo modificato per accedere alla rete in sua vece.

È possibile configurare il firewall per rilevare e bloccare i processi modificati in memoria.

Per attivare e disattivare il blocco di processi modificati:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Sulla scheda **Generale**, sotto **Blocco**, deselezionare la casella **Blocca processi se la memoria viene modificata da un'altra applicazione** per rimuovere il blocco dei processi modificati.
Per attivare il blocco di processi modificati, selezionare la relativa casella.

Se il firewall rileva un processo modificato in memoria, aggiunge delle regole per impedire al processo modificato di accedere alla rete.

Note

- Si sconsiglia di disattivare il blocco di processi modificati in maniera permanente. Disattivare il rilevamento solo quando strettamente necessario.
- Il blocco di processi modificati non è supportato sulle versioni di Windows a 64 bit.
- Viene bloccato solamente il processo modificato. Al programma che modifica il processo non viene impedito l'accesso alla rete.

7.2.13 Filtraggio dei messaggi ICMP

I messaggi di Internet Control Message Protocol (ICMP) consentono ai computer in rete di condividere informazioni relative ad errori e stato. È possibile consentire o bloccare determinati tipi di messaggi ICMP in entrata o uscita.

Filtrare i messaggi ICMP solo se in possesso di una certa competenza sui protocolli di rete. Per spiegazioni relative ai tipi di messaggi ICM, consultare la sezione [Definizione dei tipi di messaggi ICMP](#) a pagina 59.

Per filtrare i messaggi ICMP:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Nella scheda **ICMP**, selezionare la casella di spunta **Ing.** o **Usc.** per consentire i messaggi in entrata o uscita di un determinato tipo.

7.2.14 Definizione dei tipi di messaggi ICMP

Richiesta Echo, Risposta Echo	Utilizzato per verificare l'accessibilità e lo stato della destinazione. Un host invia una Richiesta Echo e attende la relativa Risposta Echo . Questa operazione viene solitamente svolta tramite il comando ping .
Destinazione irraggiungibile, Risposta Echo	Inviato dal router quando non riesce a recapitare un datagramma IP. Un datagramma è l'unità fondamentale di informazione, o pacchetto, passata attraverso una rete TCP/IP.
Quench sorgente	Inviato da un host o router se riceve dati troppo rapidamente per poterli gestire. Il messaggio è una richiesta di riduzione della velocità con cui la fonte trasmette datagrammi.
Reindirizza	Inviato da un router se riceve datagrammi che dovrebbero essere stati inviati a un router differente. Il messaggio contiene l'indirizzo a cui la fonte deve inviare i futuri datagrammi. Ciò consente di ottimizzare il routing del traffico della rete.
Annuncio del router, Sollecitazione del router	Consente agli host di scoprire l'esistenza di router. I router rendono noti periodicamente i loro indirizzi IP tramite messaggi di tipo Annuncio del router . Gli host possono richiedere l'indirizzo di un router inviando un messaggio Sollecitazione del router a cui il router risponderà con un Annuncio del router .
Tempo scaduto per un datagramma	Inviato da un router quando un datagramma ha raggiunto il livello massimo di router attraverso cui può passare.
Problema di parametro per un datagramma	Inviato da un router se si verifica un problema durante la trasmissione di un datagramma tale da non consentire il

	completamento del processo. Una possibile causa di tale problema è una non valida intestazione del datagramma.
Richiesta data e ora, Risposta data e ora	Utilizzato per sincronizzare gli orologi degli host e per fare stime sulla durata del transito.
Richiesta informazioni, Risposta informazioni	Obsoleto. In passato questi messaggi venivano utilizzati dagli host per determinare i loro indirizzi inter-network; ora sono considerati obsoleti e non dovrebbero essere utilizzati.
Richiesta maschera indirizzo, Risposta maschera indirizzo	Utilizzato per trovare la maschera della sottorete (ovvero quali parti dell'indirizzo definiscono la rete). Un host invia una Richiesta maschera indirizzo a un router e riceve una Risposta maschera indirizzo .

7.2.15 Ripristino delle impostazioni predefinite del firewall

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Gestione configurazione**, cliccare su **Ripristina predefiniti**.

7.3 Lavoro in modalità interattiva

7.3.1 Modalità interattiva

In modalità interattiva, il firewall visualizza una *finestra di apprendimento* ogni qual volta un'applicazione o servizio sconosciuti richiedono accesso alla rete. La finestra di apprendimento chiede se consentire il traffico una volta, bloccarlo una volta o se creare una regola per quel determinato tipo di traffico.

In modalità interattiva, verranno visualizzate le seguenti finestre di apprendimento:

- [Finestre di apprendimento sui processi nascosti](#) a pagina 61
- [Finestre di apprendimento sul protocollo](#) a pagina 62
- [Finestre di apprendimento sulle applicazioni](#) a pagina 62
- [Finestre di apprendimento su raw socket](#) a pagina 62
- [Finestre di apprendimento sui checksum](#) a pagina 62

7.3.2 Abilitazione della modalità interattiva

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Nella scheda **Generale**, sotto **Modalità di funzionamento**, cliccare su **Interattiva**.

7.3.3 Passaggio alla modalità non interattiva

Esistono due tipi di modalità non interattiva:

- Consenti per impostazione predefinita
- Blocca per impostazione predefinita

Nelle modalità non interattive, il firewall gestisce il traffico della rete automaticamente utilizzando le regole impostate dall'utente. Il traffico di rete che non corrisponde ad alcuna regola può essere completamente autorizzato (se in uscita) o completamente bloccato.

Per passare alla modalità interattiva:

1. Nella **Home page**, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home page**, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Nella scheda **Generale**, sotto **Modalità di funzionamento**, cliccare su **Consenti per impostazione predefinita** o **Blocca per impostazione predefinita**.

7.3.4 Finestre di apprendimento sui processi nascosti

Un processo nascosto avviene quando un'applicazione ne avvia un'altra che svolge delle operazioni di accesso alla rete per lei. Applicazioni malevole a volte utilizzano questa tecnica per aggirare i firewall; possono infatti lanciare un'applicazione ritenuta affidabile per accedere alla rete invece che tentare da sole.

La finestra di apprendimento sui processi nascosti visualizza informazioni relative al processo nascosto e all'applicazione che lo ha avviato.

- [Abilitazione delle finestre di apprendimento sui processi nascosti](#) a pagina 61

7.3.5 Abilitazione delle finestre di apprendimento sui processi nascosti

Se si utilizza la modalità interattiva, il firewall può visualizzare una finestra di apprendimento ogni qual volta rilevi una nuova applicazione di questo genere.

Se si utilizza la modalità interattiva e questa opzione non è selezionata, a queste nuove applicazioni viene impedito l'avvio di processi nascosti.

Per abilitare le finestre di apprendimento sui processi nascosti:

1. Nella **Home page**, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home page**, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Processi**.
4. Selezionare la casella di spunta **Avvisa in caso di nuove applicazioni di questo genere**.

7.3.6 Finestre di apprendimento sul protocollo

Se il firewall rileva attività di rete da parte del sistema che non riesce a relazionarsi ad alcuna applicazione specifica, richiede la creazione di una regola di protocollo.

La finestra di dialogo sul protocollo visualizza informazioni relative all'attività di rete non riconosciuta, ovvero protocollo e indirizzo remoto.

7.3.7 Finestre di apprendimento sulle applicazioni

Se il firewall rileva che un'applicazione sta tentando di accedere alla rete in una modalità non coperta da alcuna regola esistente, richiede la creazione di una regola dell'applicazione.

La finestra di apprendimento dell'applicazione visualizza informazioni relative all'attività di rete non riconosciuta, ovvero il servizio e l'indirizzo remoti.

7.3.8 Finestre di apprendimento su raw socket

I raw socket consentono ai processi di controllare tutti gli aspetti dei dati che inviano in rete e possono essere utilizzati per scopi malevoli.

Se il firewall rileva che un raw socket cerca di accedere alla rete in una modalità che non è coperta da una regola esistente, richiede la creazione di una regola sui raw socket.

La finestra di apprendimento sui raw socket visualizza informazioni relative al raw socket.

■ [Abilitazione delle finestre di apprendimento sui raw socket](#) a pagina 62

7.3.9 Abilitazione delle finestre di apprendimento sui raw socket

Se si utilizza la modalità interattiva, il firewall può visualizzare una finestra di apprendimento ogni qual volta rilevi un raw socket che tenta di accedere alla rete in una modalità non coperta da una regola esistente.

Se si utilizza la modalità interattiva e questa opzione non è selezionata, ai raw socket viene impedito l'accesso alla rete.

Per abilitare le finestre di apprendimento sui raw socket:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Processi**.
4. Selezionare la casella di spunta **Avvisa sull'utilizzo dei raw socket**.

7.3.10 Finestre di apprendimento sui checksum

Se il firewall rileva un'applicazione nuova o modificata, visualizza una finestra di apprendimento sui checksum.

Se si vuole consentire all'applicazione accesso alla rete, è necessario aggiungere all'elenco di checksum riconosciuti il suo checksum (identificatore unico).

Selezionare una delle seguenti opzioni:

- **Aggiungi il checksum a quelli esistenti per questa applicazione** consente versioni multiple dell'applicazione.
- **Sostituisci qualsiasi checksum esistente per questa applicazione** sostituisce tutti i checksum esistenti per l'applicazione con quello che richiede l'accesso e, di conseguenza, consente l'accesso solo alla versione più recente dell'applicazione.
- **Blocca questa applicazione finché non viene riavviata** in questa occasione blocca l'applicazione.

7.3.11 Abilitazione delle finestre di apprendimento sui checksum

Se si utilizza la modalità interattiva, il firewall può visualizzare una finestra di apprendimento ogni qual volta rilevi un'applicazione nuova o modificata.

Se si utilizza la modalità interattiva e questa opzione non è selezionata, alle applicazioni viene bloccato l'accesso alla rete.

Per abilitare le finestre di apprendimento sui checksum:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Sotto **Blocco**, selezionare la casella di spunta **Utilizzo di checksum per l'autenticazione delle applicazioni**.

7.4 File di configurazione firewall

7.4.1 File di configurazione del firewall

Sophos Client Firewall consente di esportare le impostazioni generali e le regole del firewall come file di configurazione. Utilizzare questa funzione per svolgere le seguenti operazioni:

- Eseguire backup e ripristino di tutte le configurazioni del firewall.
- Salvare la configurazione delle impostazioni generali ed eseguirne l'installazione in computer multipli.
- Creare le regole per le applicazioni in un solo computer ed esportarle per poi utilizzarle in altri computer che eseguono lo stesso set di applicazioni.
- Utilizzare la console di gestione per unire le configurazioni create in diversi computer per poter creare un criterio unico che sia valido per tutti i computer in rete.

7.4.2 Esportazione di un file di configurazione del firewall

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Cliccare su **Esporta**.
3. Attribuire al file di configurazione un nome e un percorso e poi cliccare su **Salva**.

7.4.3 Importazione di un file di configurazione del firewall

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Cliccare su **Importa**.
3. Selezionare un file di configurazione e cliccare su **Apri**.
4. Seguire le istruzioni sullo schermo.

7.5 Regole del firewall

7.5.1 Regole del firewall

Regole globali

Le regole globali sono applicate a tutte le comunicazioni di rete e applicazioni anche se in possesso di regole di applicazione.

Regole delle applicazioni

Un'applicazione può avere una o più regole. È possibile utilizzare sia le regole create da Sophos che creare regole personalizzate per avere pieno controllo sull'accesso consentito a un'applicazione.

7.5.2 Ordine di applicazione delle regole

Per le connessioni che utilizzano raw socket, vengono verificate solo le regole globali.

Per connessioni che *non* utilizzano raw socket, vengono verificate svariate regole, a seconda che la connessione sia verso un indirizzo di rete elencato nella scheda **LAN** o meno.

Se l'indirizzo di rete è elencato nella scheda **LAN**, vengono controllate le seguenti regole:

- Se l'indirizzo è stato contrassegnato come **Attendibile**, viene permesso tutto il traffico su tale connessione, senza ulteriori verifiche.
- Se l'indirizzo è stato contrassegnato come **NetBIOS**, viene permessa la condivisione di file e stampanti su qualsiasi connessione che rispetti i seguenti criteri:

Connessione	Porta	Intervallo
TCP	Remoto	137-139 o 445
TCP	Locale	137-139 o 445
UDP	Remoto	137 o 138
UDP	Locale	137 o 138

Se l'indirizzo di rete *non* è elencato nella scheda **LAN**, altre regole del firewall vengono verificate nel seguente ordine:

1. Tutto il traffico **NetBIOS** non consentito tramite la scheda **LAN** viene sottoposto alle seguenti procedure, a seconda delle impostazioni della casella di spunta **Blocca condivisione file e stampanti per altre reti**:
 - Se la casella è spuntata, il traffico è bloccato.
 - Se la casella non è spuntata, il traffico viene sottoposto alle restanti regole.
 2. Le regole globali ad alta priorità vengono verificate nell'ordine in cui sono elencate.
 3. Se alla connessione non sono ancora state applicate regole, vengono verificate le regole dell'applicazione.
 4. Se la connessione non è stata ancora presa in considerazione, vengono verificate le normali regole di priorità globali, secondo l'ordine in cui sono elencate.
 5. Se non è stata rilevata alcuna regola per la gestione della connessione:
 - Nella modalità **Consenti per impostazione predefinita** il traffico viene consentito (se si tratta di traffico in uscita).
 - Nella modalità **Blocca per impostazione predefinita**, viene bloccato il traffico.
 - Nella modalità **Interattiva**, l'utente deve decidere.
- Nota:** Se la modalità di funzionamento non è stata modificata, il firewall sarà in modalità **Blocca per impostazione predefinita**.

7.5.3 Rilevamento della rete locale

È possibile assegnare regole del firewall alla rete locale del computer.

Il firewall determina la rete locale di questo computer al momento del suo avvio, e controlla qualsiasi cambiamento mentre è acceso. Se viene rilevata qualsiasi modifica, il firewall aggiorna le regole della rete locale con l'intervallo di indirizzi della nuova rete locale.



Attenzione: Consigliamo vivamente di esercitare cautela quando si utilizzano le regole della rete locale come parte di configurazioni utilizzabili "da fuori ufficio". Per ulteriori informazioni, consultare la sezione [Creazione di una configurazione secondaria](#) a pagina 74.

7.5.4 Regole globali

7.5.4.1 Impostazioni delle regole globali predefinite

Qui vengono descritte le condizioni e le azioni per le regole globali predefinite. Utilizzare queste impostazioni, se si desidera creare una nuova regola globale predefinita.

Consenti DNS Resolving (TCP)

- Protocollo: TCP
- Direzione: in uscita
- Porta remota: DOMAIN
- Azione: consenti

Consenti DNS Resolving (UDP)

- Protocollo: UDP
- Direzione: in uscita
- Porta remota: DNS
- Azione: consenti Stateful inspection

Consenti DHCP in uscita

- Protocollo: UDP
- Porta locale: BOOTPS,BOOTPC,546,547
- Azione: consenti

Consenti identificazione in entrata

- Protocollo: TCP
- Direzione: in entrata
- Porta locale: AUTH
- Azione: consenti

Consenti Loopback

- Protocollo: TCP
- Direzione: in entrata
- Porta locale: 127.0.0.0 (255.255.255.0)
- Azione: consenti

Consenti Protocollo GRE

- Protocollo: TCP
- Tipo di protocollo: in uscita
- Azione: consenti

Consenti connessione di controllo PPTP

- Protocollo: TCP
- Direzione: in uscita
- Porta remota: PPTP
- Porta locale: 1024-65535
- Azione: consenti

Blocca chiamata RPC (TCP)

- Protocollo: TCP
- Direzione: in entrata
- Porta locale: DCOM
- Azione: blocca

Blocca chiamata RPC (UDP)

- Protocollo: UDP
- Porta locale: 135
- Azione: blocca

Blocca Protocollo Server Message Block (TCP)

- Protocollo: TCP
- Direzione: in entrata
- Porta locale: MICROSOFT_DS
- Azione: blocca

Blocca Protocollo Server Message (UDP)

- Protocollo: TCP
- Porta locale: 445
- Azione: blocca

Consenti Connessione UDP a Localhost

- Protocollo: UDP
- Host remoto: 255.255.255.255 (0.0.0.0)
- Host locale: 255.255.255.255 (0.0.0.0)
- Dove la porta locale è uguale alla porta remota: true
- Azione: consenti

7.5.4.2 Creazione di una regola globale

Importante: Sophos consiglia di modificare regole globali solo se in possesso di una certa competenza sui protocolli di rete.

Le regole globali vengono applicate a tutte le comunicazioni della rete e a tutte le applicazioni non ancora in possesso di una regola specifica.

Per creare una regola globale:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Regole globali**.
4. Cliccare su **Aggiungi**.
5. Sotto **Nome della regola**, digitare il nome della regola.
Il nome della regola deve essere unico all'interno dell'elenco delle regole. Due regole globali non possono avere lo stesso nome.
6. Per applicare la regola prima di qualsiasi regola dell'applicazione o del normale ordine di priorità delle regole globali, selezionare la casella di spunta **Regola con elevata priorità**.
Per ulteriori informazioni sull'ordine di applicazione delle regole, consultare la sezione [Ordine di applicazione delle regole](#) a pagina 64.
7. Sotto **Seleziona gli eventi che saranno gestiti dalla regola**, selezionare le condizioni che la connessione deve rispettare affinché la regola venga applicata.
8. Sotto **Seleziona le azioni alle quali la regola reagirà**, selezionare **Consenti** o **Blocca**.
9. Effettuare una delle seguenti operazioni:
 - Per consentire altre connessioni da e verso lo stesso indirizzo remoto mentre la connessione iniziale è ancora attiva, selezionare **Connessioni concorrenti**.
Nota: Questa opzione è disponibile solo per le regole TCP, che sono di stato per impostazione predefinita.
 - Per consentire risposte intelligenti dal computer remoto in base alla connessione iniziale, selezionare **Ispezione di stato**.
10. Sotto **Descrizione della regola**, cliccare su un valore sottolineato. Per esempio, se si clicca sul link **TCP** si apre la finestra di dialogo **Seleziona protocollo**.

7.5.4.3 Modifica di una regola globale

Importante: Sophos consiglia di modificare regole globali solo se in possesso di una certa competenza sui protocolli di rete.

Per modifica una regola globale:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Regole globali**.
4. Nell'elenco **Regola**, scegliere la regola che si desidera modificare.
5. Cliccare su **Modifica**.
Per informazioni sulle impostazioni delle regole globali, consultare la sezione [Creazione di una regola globale](#) a pagina 67.

7.5.4.4 Copia di una regola globale

Per copiare una regola globale e aggiungerla all'elenco delle regole:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Regole globali**.
4. Nell'elenco **Regola**, scegliere la regola che si desidera copiare.
5. Cliccare su **Copia**.

7.5.4.5 Cancellazione di una regola globale

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Regole globali**.
4. Nell'elenco **Regola**, scegliere la regola che si desidera cancellare.
5. Cliccare su **Rimuovi**.

7.5.4.6 Modifica dell'ordine di applicazione delle regole globali

Le regole globali vengono applicate secondo l'ordine in cui appaiono nell'elenco delle regole, dall'alto verso il basso.

Per modificare l'ordine di applicazione delle regole globali:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Regole globali**.
4. Nell'elenco **Regola**, cliccare sulla regola che si desidera spostare in alto o in basso nell'elenco.
5. Cliccare su **Sposta su** o **Sposta giù**.

7.5.5 Regole delle applicazioni

7.5.5.1 Applicazione delle regole delle applicazioni predefinite

Si tratta di una serie di regole delle applicazioni create da Sophos. Per aggiungere regole predefinite all'elenco di regole per un'applicazione:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Applicazioni**.
4. Select the application in the list, and then click the arrow next to **Personalizza** .
5. Andare a **Aggiungi regole da quelle predefinite** e cliccare sulla regola predefinita.

7.5.5.2 Creazione di una regola dell'applicazione

Per creare una regola personalizzata che rappresenti un buon meccanismo di controllo sulla concessione dell'accesso a una determinata applicazione:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Applicazioni**.
4. Selezionare l'applicazione nell'elenco e cliccare su **Personalizza**.
È anche possibile cliccare due volte sull'applicazione nell'elenco.
5. Nella finestra di dialogo **Regole applicazioni**, cliccare su **Aggiungi**.
6. Sotto **Nome della regola**, digitare il nome della regola.
Il nome della regola deve essere unico all'interno dell'elenco delle regole. Due regole delle applicazioni non possono avere lo stesso nome, ma due applicazioni possono avere ciascuna una regola con lo stesso nome.
7. Sotto **Seleziona gli eventi che saranno gestiti dalla regola**, selezionare le condizioni che la connessione deve rispettare affinché la regola venga applicata.
8. Sotto **Seleziona le azioni alle quali la regola reagirà**, selezionare **Consenti** o **Blocca**.
9. Per consentire risposte intelligenti dal computer remoto in base alla connessione iniziale, selezionare **Ispezione di stato**.
10. Sotto **Descrizione della regola**, cliccare su un valore sottolineato. Per esempio, se si clicca sul link **TCP** si apre la finestra di dialogo **Seleziona protocollo**.

7.5.5.3 Modifica di una regola delle applicazioni

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Applicazioni**.
4. Selezionare l'applicazione nell'elenco e cliccare su **Personalizza**.
È anche possibile cliccare due volte sull'applicazione nell'elenco.
5. Nella finestra di dialogo **Regole applicazioni**, cliccare su **Modifica**.
6. Sotto **Nome della regola**, digitare il nome della regola.
Il nome della regola deve essere unico all'interno dell'elenco delle regole. Due regole delle applicazioni non possono avere lo stesso nome, ma due applicazioni possono avere ciascuna una regola con lo stesso nome.
7. Sotto **Seleziona gli eventi che saranno gestiti dalla regola**, selezionare le condizioni che la connessione deve rispettare affinché la regola venga applicata.
8. Sotto **Seleziona le azioni alle quali la regola reagirà**, selezionare **Consenti** o **Blocca**.
9. Per consentire risposte intelligenti dal computer remoto in base alla connessione iniziale, selezionare **Ispezione di stato**.
10. Sotto **Descrizione della regola**, cliccare su un valore sottolineato. Per esempio, se si clicca sul link **TCP** si apre la finestra di dialogo **Seleziona protocollo**.

7.5.5.4 Copia di una regola delle applicazioni

Per copiare una regola delle applicazioni e aggiungerla all'elenco delle regole:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Applicazioni**.
4. Selezionare l'applicazione nell'elenco e cliccare su **Personalizza**.
È anche possibile cliccare due volte sull'applicazione nell'elenco.
5. Nella finestra di dialogo **Regole applicazioni**, cliccare su **Copia**.

7.5.5.5 Cancellazione di una regola delle applicazioni

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Applicazioni**.
4. Selezionare l'applicazione nell'elenco e cliccare su **Personalizza**.
5. Nella finestra di dialogo **Regole applicazioni**, cliccare su **Rimuovi**.

7.5.5.6 Modifica dell'ordine di applicazione delle regole delle applicazioni

Le regole dell'applicazione vengono applicate secondo l'ordine in cui appaiono nell'elenco delle regole, dall'alto verso il basso.

Per modificare l'ordine di applicazione delle regole delle applicazioni:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Applicazioni**.
4. Selezionare l'applicazione nell'elenco e cliccare su **Personalizza**.
È anche possibile cliccare due volte sull'applicazione nell'elenco.
5. Nell'elenco **Regola**, cliccare sulla regola che si desidera spostare in alto o in basso nell'elenco.
6. Cliccare su **Sposta su** o **Sposta giù**.

7.5.5.7 Autorizzazione dell'avvio di processi nascosti

Un'applicazione a volte ne avvia un'altra che svolge delle operazioni di accesso alla rete per lei.

Applicazioni malevole possono utilizzare questa tecnica per aggirare i firewall; possono infatti lanciare un'applicazione ritenuta affidabile per accedere alla rete invece che tentare da sole.

Il firewall invia un allarme alla console di gestione, se se ne sta utilizzando una, la prima volta che viene rilevato un processo nascosto.

Per consentire l'avvio di processi nascosti:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Processi**.
4. Nell'area in alto, cliccare sul pulsante **Aggiungi**.
5. Trovare l'applicazione e cliccarvi due volte.

Se si utilizza la modalità interattiva, il firewall può visualizzare una finestra di apprendimento ogni qual volta rilevi una nuova applicazione di questo genere.

- [Abilitazione della modalità interattiva](#) a pagina 60
- [Abilitazione delle finestre di apprendimento sui processi nascosti](#) a pagina 61

7.5.5.8 Autorizzazione dell'utilizzo di raw socket da parte di applicazioni

Alcune applicazioni possono accedere alla rete tramite raw socket che forniscono loro controllo su tutti gli aspetti relativi ai dati inviati nella rete.

Alcune applicazioni malevole possono sfruttare i raw socket contraffacendo il loro indirizzo IP o inviando messaggi volutamente corrotti.

Nel caso ne venga utilizzato uno, il firewall invia un allarme alla console di gestione la prima volta che rileva un raw socket.

Per consentire alle applicazioni di accedere alla rete tramite raw socket:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Processi**.
4. Nell'area in basso, cliccare sul pulsante **Aggiungi**.
5. Trovare l'applicazione e cliccarvi due volte.

Se si utilizza la modalità interattiva, il firewall può visualizzare una finestra di apprendimento ogni qual volta rilevi un raw socket.

- [Abilitazione della modalità interattiva](#) a pagina 60
- [Abilitazione delle finestre di apprendimento sui raw socket](#) a pagina 62

7.5.5.9 Utilizzo di checksum per l'autenticazione di applicazioni

Ogni versione di un'applicazione ha un checksum unico. Il firewall può utilizzare tale checksum per decidere se un'applicazione è consentita o meno.

Per impostazione predefinita, il firewall verifica il checksum di tutte le applicazioni in esecuzione. Se il checksum non è noto o è stato modificato, il firewall lo blocca o (in modalità interattiva) chiede all'utente come procedere.

Il firewall invia anche un allarme alla console di gestione, se ne viene utilizzata una, la prima volta che rileva un'applicazione nuova o modificata.

Per aggiungere un checksum all'elenco di checksum autorizzati:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Cliccare sulla scheda **Checksum**.
4. Cliccare su **Aggiungi**.
5. Trovare l'applicazione e cliccarvi due volte.

Se si utilizza la modalità interattiva, il firewall può visualizzare una finestra di apprendimento ogni qual volta rilevi un'applicazione nuova o modificata.

- [Abilitazione della modalità interattiva](#) a pagina 60
- [Abilitazione delle finestre di apprendimento sui processi nascosti](#) a pagina 61

7.6 Riconoscimento presenza

7.6.1 Riconoscimento della presenza in rete

Il riconoscimento della presenza in rete è una funzionalità di Sophos Client Firewall che attribuisce una configurazione del firewall a ciascuna scheda di rete presente sul computer, a seconda dell'attuale posizione della scheda di rete stessa.

Lo scenario più consueto per l'utilizzo di tale funzionalità si presenta quando si è in possesso di un laptop aziendale, e si lavora dalla propria abitazione. Si utilizzano così due connessioni di rete allo stesso momento:

- Per il lavoro, ci si connette alla rete aziendale mediante un client VPN ed una **scheda di rete virtuale**.
- Per uso personale, ci si connette al proprio internet service provider tramite un cavo di rete ed una **scheda di rete fisica**.

In questo scenario, occorre che la configurazione lavorativa venga applicata alla connessione aziendale virtuale, e che la configurazione non lavorativa (di solito più restrittiva) venga applicata alla connessione del provider di servizi internet non lavorativo.

Nota: La configurazione non lavorativa richiederà che siano presenti abbastanza regole per consentire alla connessione aziendale "virtuale" di essere stabilita.

7.6.2 Impostazione del riconoscimento della presenza in rete

1. Definire l'elenco di indirizzi o domini gateway di MAC dei propri percorsi primari. Di norma, si tratta delle proprie reti aziendali.
2. Creare la configurazione del firewall che verrà utilizzata per i propri percorsi primari. Di solito tale configurazione è meno restrittiva.
3. Creazione di una configurazione secondaria. Di solito tale configurazione è più restrittiva.
4. Selezionare una configurazione da applicare.

A seconda del metodo di rilevamento utilizzato, il firewall ottiene l'indirizzo DNS o gateway per ciascuna scheda di rete del computer, e le paragona all'elenco di indirizzi fornito.

- Se si verifica una corrispondenza fra uno degli indirizzi nell'elenco e l'indirizzo di una scheda di rete, a tale scheda viene assegnata la configurazione per il **percorso primario**.
- Se non si verifica alcuna corrispondenza gli indirizzi nell'elenco e quelli delle schede di rete, alla scheda viene assegnato il criterio per il **percorso secondario**.

Il percorso attivo è visualizzato nel pannello **Stato** della finestra **Sophos Endpoint Security and Control**. Se sono state applicate entrambi le configurazioni, **Attivo = Entrambi**.

Importante: La configurazione secondaria passa dalla modalità **Interattiva** a quella **Blocca per impostazione predefinita** quando si verificano entrambe le seguenti condizioni:

- Entrambi i percorsi sono attivi.
- La configurazione primaria *non* è interattiva.

7.6.3 Definizione dei percorsi primari

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Cliccare sulla scheda **Rilevamento percorso**.
3. Sotto **Metodo di rilevamento**, cliccare su **Configura** di fianco al metodo che si desidera utilizzare per definire i percorsi primari:

Opzione	Descrizione
Identifica percorso tramite DNS	Creazione di un elenco di nomi di dominio e indirizzi IP previsti, corrispondenti ai percorsi primari.
Identifica percorso tramite indirizzi gateway MAC	Creazione di un elenco di indirizzi gateway MAC corrispondenti ai percorsi primari.

4. Seguire le istruzioni sullo schermo.

7.6.4 Creazione di una configurazione secondaria

Il firewall utilizza la configurazione secondaria quando non si è connessi a un percorso primario.

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Selezionare la casella di spunta **Aggiungi configurazione per percorso secondario**.

Impostare ora la configurazione per il percorso secondario. Per informazioni su come svolgere questa operazione, riferirsi a [Configurazione del firewall](#) a pagina 53 e agli altri argomenti nella sezione [Configurazione del firewall](#).



Attenzione: Se il computer è un laptop, e viene utilizzato all'esterno dell'ufficio, esiste la possibilità che si colleghi ad una rete locale sconosciuta. In tale evenienza, le regole del firewall

nella configurazione secondaria che utilizzano la rete locale come indirizzo possono inavvertitamente consentire traffico sconosciuto. Per questo motivo, si consiglia vivamente di esercitare cautela quando si utilizzano le regole di rete locale come parte di configurazioni secondarie.

7.6.5 Selezione di una configurazione da applicare

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nella scheda **Generale**, sotto **Percorso applicato**, cliccare su una delle seguenti opzioni:

Opzione	Descrizione
Applica la configurazione per il percorso rilevato	Il firewall applica la configurazione primaria o secondaria a ciascuna connessione di rete, a seconda delle impostazioni di rilevamento per il riconoscimento della presenza in rete (come descritto nella sezione Impostazione del riconoscimento della presenza in rete a pagina 73).
Applica la configurazione per il percorso primario	Il firewall applica la configurazione primaria a tutte le connessioni di rete.
Applica la configurazione per il percorso secondario	Il firewall applica la configurazione secondaria a tutte le connessioni di rete.

7.7 Reportistica del firewall

7.7.1 Reportistica del firewall

Per impostazione predefinita, i report del firewall comunicano alla console di gestione cambiamenti di stato, eventi ed errori.

Cambiamenti di stato del firewall

Il firewall considera cambiamenti di stato i cambiamenti riportati di seguito:

- Cambiamenti delle modalità di funzionamento
- Cambiamenti della versione del software
- Cambiamenti della configurazione del firewall per autorizzare tutto il traffico
- Cambiamenti della conformità del firewall al criterio

Quando si lavora in modalità interattiva, la configurazione firewall potrebbe essere deliberatamente diversa dal criterio applicato dalla console di gestione. Se questo è il caso, è possibile decidere di **non** inviare alla console di gestione allarmi "diverso dal criterio", quando si apportano cambiamenti a determinate parti della configurazione del firewall.

Per ulteriori informazioni, consultare la sezione [Attivazione o disattivazione del rilevamento di modifiche locali](#) a pagina 76.

Eventi firewall

Un *evento* si verifica quando un'applicazione sconosciuta nel computer, o il sistema operativo del computer, prova a comunicare con un altro computer tramite una connessione di rete.

È possibile impedire che il firewall riporti alla console di gestione gli eventi.

Per ulteriori informazioni, consultare la sezione [Disattivazione del rilevamento del traffico di rete sconosciuto](#) a pagina 76.

7.7.2 Attivazione o disattivazione del rilevamento di modifiche locali

Se la configurazione del firewall differisce dal criterio, è possibile **disattivare il rilevamento di modifiche locali**.

La disattivazione del rilevamento di modifiche locali fa in modo che il firewall non invii allarmi "diverso dal criterio" alla console di gestione in relazione alle modifiche apportate a regole globali, applicazioni, processi o checksum. Scegliere questa opzione quando si lavora in modalità interattiva, dal momento che si tratta di impostazioni modificabili tramite finestre di apprendimento.

Se nel computer la configurazione del firewall deve essere conforme al criterio, si dovrà **attivare il rilevamento di modifiche locali**.

Per disattivare il rilevamento di modifiche locali:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Nella scheda **Generale**, sotto **Reportistica**, per disattivare il rilevamento di modifiche locali, deselezionare la casella di spunta **Visualizza un allarme nella console di gestione se a regole globali, applicazioni, processi o checksum sono apportate modifiche a livello locale**.

Per attivare il rilevamento di modifiche locali, selezionare la casella di spunta.

7.7.3 Disattivazione del rilevamento del traffico di rete sconosciuto

È possibile impedire che il firewall riporti alla console di gestione il traffico di rete sconosciuto. Il firewall considera il traffico sconosciuto se non rileva regole relative ad esso.

Per impedire che il firewall riporti alla console di gestione il traffico di rete sconosciuto:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Nella scheda **Generale**, sotto **Blocco**, selezionare la casella di spunta **Utilizzo di checksum per l'autenticazione delle applicazioni**.

4. Sotto **Reportistica**, deselezionare la casella di spunta **Segnala le applicazioni sconosciute e il traffico alla console di gestione**.

7.7.4 Disattivazione del rilevamento degli errori del firewall

Importante: Si sconsiglia la disattivazione permanente del rilevamento degli errori del firewall. Disattivare il rilevamento solo quando strettamente necessario.

Per impedire che il firewall riporti errori alla console di gestione:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Nella scheda **Generale**, sotto **Reportistica**, deselezionare la casella di spunta **Segnala errori alla console di gestione**.

7.7.5 Configurazione della messaggistica desktop

È possibile controllare quali messaggi il firewall visualizzi nel desktop tramite l'utilizzo di fumetti.

Fumetti relativi ad applicazioni sconosciute e traffico non vengono mostrati in modalità interattiva dal momento che le stesse informazioni vengono visualizzate nelle finestre di apprendimento.

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Sotto **Configurazioni**, cliccare su **Configura** di fianco al percorso che si desidera configurare.
3. Nella scheda **Generale**, sotto **Messaggistica desktop**, svolgere una delle seguenti operazioni:
 - Per visualizzare i fumetti relativi ad allarmi ed errori del firewall, selezionare la casella di spunta **Mostra allarmi ed errori**.
 - Per visualizzare i fumetti relativi ad applicazioni sconosciute e traffico, selezionare la casella di spunta **Mostra applicazioni sconosciute e traffico**.

7.8 Log firewall

7.8.1 Visualizzatore del log del firewall

Il visualizzatore del log di Sophos Client Firewall consente di visualizzare, filtrare e salvare dettagli relativi a:

- Tutte le connessioni
- Connessioni che sono state consentite o bloccate
- Eventi firewall
- Log di sistema

7.8.2 Apertura del visualizzatore del log del firewall

- ❖ Nella **Home** page, sotto **Firewall**, cliccare su **Visualizza log firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.

7.8.3 Configurazione del log del firewall

Per gestire la dimensione e i contenuti del database del log eventi del firewall:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Configurazione firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Cliccare sulla scheda **Log**.
3. Per gestire la dimensione del database del log eventi del firewall, selezionare una delle seguenti opzioni:
 - Per consentire al database di crescere senza alcun limite, cliccare su **Mantieni tutti i record**.
 - Per cancellare i vecchi record, cliccare su **Elimina i record vecchi**, e poi configurare le **Impostazioni cancellazione log**.
4. Sotto **Impostazioni cancellazione log**, selezionare una o più delle seguenti opzioni:
 - Cliccare sulla casella di spunta **Elimina i record dopo**, e successivamente inserire o selezionare un numero nella casella **Giorni**.
 - Cliccare sulla casella di spunta **Mantieni non più di**, e successivamente inserire o selezionare un numero nella casella **Record**.
 - Cliccare sulla casella di spunta **Mantieni dimensioni entro**, e successivamente inserire o selezionare un numero nella casella **MB**.

7.8.4 Modifica dell'aspetto del visualizzatore del log del firewall

1. Nella **Home** page, sotto **Firewall**, cliccare su **Visualizza log firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Dal menu **Visualizza**, cliccare su **Layout**.
3. Nella finestra di dialogo **Visualizza personalizzazione**, selezionare gli oggetti che si desidera nascondere o visualizzare:
 - L'**Albero della console** viene visualizzato nel riquadro a sinistra.
 - La **Barra degli strumenti** viene visualizzata nella parte alta del visualizzatore del log del firewall.
 - La **Barra delle descrizioni** viene visualizzata sopra i dati nel riquadro a destra.
 - La **Barra di stato** viene visualizzata nella parte bassa del visualizzatore del log del firewall.

7.8.5 Personalizzazione del formato dei dati

È possibile cambiare il formato utilizzato per visualizzare i seguenti oggetti relativi ai dati nei log del firewall:

- Visualizzare le porte sotto forma di numero o nome, per es. **HTTP** o **80**.
- Visualizzare le applicazioni come icone, percorsi file o entrambi.
- Specificare l'unità di misura utilizzata per visualizzare i dati relativi alla velocità del trasferimento dei dati, per es. **KByte** o **MByte**.
- Nascondere o visualizzare griglie

Per personalizzare il formato dei dati:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Visualizza log firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Dal menu **Visualizza**, cliccare su **Personalizza**.
3. Selezionare le opzioni desiderate.

7.8.6 Mostra o nascondi colonne nel visualizzatore del log del firewall

1. Nella **Home** page, sotto **Firewall**, cliccare su **Visualizza log firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Cliccare su un oggetto nell'albero della console che visualizzi colonne nel riquadro dei dettagli.
3. Nel menu **Visualizza**, selezionare **Aggiungi/rimuovi colonne**.
È anche possibile cliccare col tasto destro del mouse su tutte le intestazioni delle colonne.
4. Nella finestra di dialogo **Colonne**, svolgere una delle seguenti operazioni:
 - Per nascondere una colonna, deselezionare la relativa casella di spunta.
 - Per visualizzare una colonna, selezionare la relativa casella di spunta.

7.8.7 Riordinamento delle colonne nel visualizzatore del log del firewall

1. Nella **Home** page, sotto **Firewall**, cliccare su **Visualizza log firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Cliccare su un oggetto nell'albero della console che visualizzi colonne nel riquadro dei dettagli.
3. Nel menu **Visualizza**, selezionare **Aggiungi/rimuovi colonne**.
È anche possibile cliccare col tasto destro del mouse su tutte le intestazioni delle colonne.
4. Nella finestra di dialogo **Colonne**, cliccare sul nome di una colonna e poi su **Sposta su** o **Sposta giù** per cambiare la posizione della colonna.

Note

- È inoltre possibile riordinare le colonne nel riquadro dei dettagli utilizzando il mouse e trascinando l'intestazione della colonna a destra o sinistra della sua posizione originale. Quando si trascina una colonna, parti evidenziate tra le intestazioni delle colonne indicano la nuova posizione della colonna.
- È possibile cambiare le dimensioni delle colonne utilizzando il mouse per trascinare le intestazioni delle colonne.

7.8.8 Filtraggio dei record in un log del firewall

È possibile classificare i record del log del firewall creando un filtro.

Per filtrare i record del log del firewall:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Visualizza log firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nell'albero della console, selezionare un log.
3. Nel menu **Azione**, cliccare su **Aggiungi filtro**.
4. Seguire le istruzioni della procedura guidata **Filtro**.

Il filtro appare nell'albero della console immediatamente sotto al nodo che si desiderava filtrare.

7.8.9 Esportazione di tutti i record da un log del firewall

Per esportare tutti i record dal log del firewall a un file di testo o CSV:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Visualizza log firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nell'albero della console, selezionare un log.
3. Cliccare col tasto destro del mouse sull'elenco dei record e poi cliccare su **Esporta tutti i record**.
4. Nel campo di testo **Nome file**, digitare un nome per il file.
5. Nell'elenco **Salva come**, cliccare sul tipo di file desiderato.

7.8.10 Esportazione di record selezionati da un log del firewall

Per esportare record selezionati da un log del firewall a un file di testo o CSV:

1. Nella **Home** page, sotto **Firewall**, cliccare su **Visualizza log firewall**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nell'albero della console, selezionare un log.
3. Selezionare i record che si desidera esportare.
Se i record si aggiornano rapidamente, nel menu **Visualizza**, deselezionare la casella di spunta **Aggiornamento automatico**.
4. Nel menu **Azione**, cliccare su **Esporta record selezionati**.

5. Nel campo di testo **Nome file**, digitare un nome per il file.
6. Nell'elenco **Salva come**, cliccare sul tipo di file desiderato.

8 Sophos AutoUpdate

8.1 Aggiornamento immediato

Per impostazione predefinita, Sophos AutoUpdate è programmato per aggiornarsi ogni 10 minuti se si è costantemente collegati alla rete aziendale, o ogni 60 minuti se si è continuamente collegati ad internet.

Se si è in possesso di una connessione di tipo dial-up, Sophos AutoUpdate è impostato per eseguire gli aggiornamenti ogni qual volta connessi a Internet o alla rete, dopodiché ogni 60 minuti.

Per eseguire aggiornamenti immediati:

- ❖ Cliccare col tasto destro del mouse sull'icona nell'area di notifica di Sophos Endpoint Security and Control e poi cliccare su **Aggiorna ora**.

8.2 Pianificazione degli aggiornamenti

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

È possibile specificare la modalità o la frequenza degli aggiornamenti di Sophos AutoUpdate.

1. Nel menu **Configura**, cliccare su **Aggiornamento**.
2. Cliccare sulla scheda **Pianificazione**
3. Selezionare **Consenti aggiornamenti automatici** ed inserire la frequenza (in minuti) con la quale Sophos AutoUpdate eseguirà gli aggiornamenti.
Se l'aggiornamento dei file viene scaricato dalla rete aziendale, gli aggiornamenti avvengono ogni 10 minuti per impostazione predefinita.
Se l'aggiornamento dei file viene scaricato tramite internet dal server di Sophos, Sophos AutoUpdate può svolgere gli aggiornamenti con una frequenza massima di 60 minuti.

8.3 Impostazione di una fonte per gli aggiornamenti

Se si desidera che Sophos AutoUpdate esegua l'aggiornamento automatico, è necessario specificare la fonte da cui scaricare gli aggiornamenti.

1. Nel menu **Configura**, cliccare su **Aggiornamento**.
2. Cliccare sulla scheda **Percorso primario**.
3. Nell'elenco **Indirizzo**, inserire il percorso UNC o l'indirizzo web del server di aggiornamento.
Per scaricare gli aggiornamenti direttamente da Sophos tramite Internet, selezionare **Sophos** dall'elenco **Indirizzo**.
4. Nella casella **Nome utente**, digitare il Nome utente per l'account utilizzato per accedere al server di aggiornamento.
Se il Nome utente deve riportare il dominio, utilizzare la forma *dominio\nome utente*.

5. Nella casella **Password**, digitare la password dell'account utilizzato per accedere al server di aggiornamento.

8.4 Impostazione di una fonte alternativa per gli aggiornamenti

È possibile impostare una fonte alternativa per gli aggiornamenti. Se Sophos AutoUpdate non riesce ad eseguire gli aggiornamenti dalla fonte consueta, tenterà di farlo da quella alternativa.

1. Nel menu **Configura**, cliccare su **Aggiornamento**.
2. Cliccare sulla scheda **Percorso secondario**.
3. Nell'elenco **Indirizzo**, inserire il percorso UNC o l'indirizzo web del server di aggiornamento.
Per scaricare gli aggiornamenti direttamente da Sophos tramite Internet, selezionare **Sophos** dall'elenco **Indirizzo**.
4. Nella casella **Nome utente**, digitare il Nome utente per l'account utilizzato per accedere al server di aggiornamento.
Se il Nome utente deve riportare il dominio, utilizzare la forma *dominio\nome utente*.
5. Nella casella **Password**, digitare la password dell'account utilizzato per accedere al server di aggiornamento.

8.5 Aggiornamento tramite server proxy

Se Sophos AutoUpdate esegue gli aggiornamenti via Internet, è necessario inserire i dati del server proxy utilizzato per connettersi a Internet.

1. Nel menu **Configura**, cliccare su **Aggiornamento**.
2. Cliccare sulla scheda **Percorso primario** o **Percorso secondario**.
3. Cliccare su **Dati proxy**.
4. Selezionare la casella di spunta **Accedi al percorso tramite proxy**.
5. Inserire l'**Indirizzo** e il numero di **Porta** del server proxy.
6. Inserire il **Nome utente** e la **Password** che danno accesso al server proxy.
Se il Nome utente deve riportare il dominio, utilizzare la forma *dominio\nome utente*.

8.6 Aggiornamento tramite connessione dial-up

Per eseguire gli aggiornamenti tramite connessione dial-up a Internet:

1. Nel menu **Configura**, cliccare su **Aggiornamento**.
2. Cliccare sulla scheda **Pianificazione**
3. Selezionare **Verifica la disponibilità di aggiornamenti in fase di connessione**.

Sophos AutoUpdate esegue l'aggiornamento ogni qual volta ci si connetta a Internet.

8.7 Limitazione della larghezza di banda utilizzata per gli aggiornamenti

Per evitare che Sophos AutoUpdate occupi tutta la larghezza di banda quando è invece necessaria per altri motivi (quali scaricare la posta elettronica), è possibile limitarne la quantità utilizzata.

1. Nel menu **Configura**, cliccare su **Aggiornamento**.
2. Cliccare sulla scheda **Percorso primario** o **Percorso secondario**.
3. Cliccare su **Avanzate**.
4. Selezionare la casella di spunta **Limita occupazione di banda** e spostare l'indicatore in modo tale da indicare la quantità di larghezza di banda che Sophos AutoUpdate potrà utilizzare.

Nota: se si specifica una larghezza di banda superiore alla quantità disponibile, Sophos AutoUpdate utilizzerà tutta la larghezza di banda.

8.8 Log dell'attività di aggiornamento

È possibile configurare Sophos AutoUpdate in modo tale che registri l'attività di aggiornamento in un file di log.

1. Nel menu **Configura**, cliccare su **Aggiornamento**.
2. Cliccare sulla scheda **Log**.
3. Selezionare la casella di spunta **Crea log dell'attività di Sophos AutoUpdate**.
4. Nella casella **Dimensioni massime log**, digitare o selezionare la dimensione massima in MB del log.
5. Nell'elenco **Livello di log**, selezionare un log **Normale** o **Dettagliato**.

Il log dettagliato fornisce informazioni su molte più attività del normale, quindi il log si riempirà più rapidamente. Utilizzare questa opzione solo quando è necessario un log dettagliato per la risoluzione dei problemi.

8.9 Visualizzazione del file di log degli aggiornamenti

1. Nel menu **Configura**, cliccare su **Aggiornamento**.
2. Cliccare sulla scheda **Log**.
3. Cliccare su **Visualizza file di log**.

9 Sophos Tamper Protection

9.1 Il blocco rimozione in questo computer

Il blocco rimozione consente di impedire a malware noto e utenti non autorizzati (amministratori locali e utenti con conoscenze tecniche limitate), la disinstallazione del software di sicurezza Sophos o la disabilitazione tramite l'interfaccia Sophos Endpoint Security and Control.

Nota: Il blocco rimozione non è pensato per offrire protezione contro utenti con vaste conoscenze tecniche. Non offre protezione contro malware appositamente studiato per sabotare il rilevamento da parte del sistema operativo. Tale tipo di malware può essere rilevato solamente eseguendo una scansione alla ricerca di minacce e comportamenti sospetti. (Per ulteriori informazioni, consultare la sezione "Utilizzo di Sophos Anti-Virus").

Cosa implica il blocco rimozione per gli utenti del computer?

SophosUsers e SophosPowerUsers

Il blocco rimozione non influisce sui gruppi SophosUsers e SophosPowerUsers. Quando il blocco rimozione è attivo, essi potranno comunque eseguire tutte le operazioni alle quali sono normalmente autorizzati, senza bisogno di immettere la password del blocco rimozione.

SophosUsers o SophosPowerUsers non possono attivare o disattivare il blocco rimozione.

Per maggiori informazioni sulle operazioni che ciascun gruppo Sophos è autorizzato ad effettuare, consultare la sezione [Gruppi Sophos](#) a pagina 5.

SophosAdministrators

I membri del gruppo SophosAdministrator sono autorizzati ad abilitare e disabilitare il blocco rimozione.

Se su questo computer viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control, i criteri del blocco rimozione impostati nella console determinano la configurazione e la password del blocco rimozione. Se il blocco rimozione viene abilitato dalla console, chiedere la password al proprio amministratore se occorre eseguire una delle operazioni menzionate qui di seguito.

I membri del gruppo SophosAdministrator devono conoscere la password del blocco rimozione, se il blocco rimozione è abilitato, per effettuare le seguenti operazioni:

- Riconfigurare le impostazioni della scansione in accesso o del rilevamento di comportamenti sospetti in Sophos Endpoint Security and Control. Per ulteriori informazioni, consultare la sezione [Inserimento della password del blocco rimozione per configurare il software](#) a pagina 87.
- Disabilitare il blocco rimozione Per ulteriori informazioni, consultare la sezione [Disabilitazione del blocco rimozione](#) a pagina 86.
- Disinstallare i componenti di Sophos Endpoint Security and Control (Sophos Anti-Virus, Sophos Client Firewall, Sophos AutoUpdate, Sophos Remote Management System), utilizzando il Pannello di Controllo.
- Disinstallare Sophos SafeGuard Disk Encryption utilizzando il Pannello di Controllo.

Un SophosAdministrator che non conosce la password potrà eseguire tutte le altre operazioni, eccetto quelle menzionate sopra.

Se il blocco rimozione non è attivo, ma la password del blocco rimozione è già stata impostata, è necessario utilizzare l'opzione **Autentica utente** per autenticarsi prima di poter riattivare il blocco rimozione. Quando il blocco rimozione non è attivo, sono abilitate tutte le altre opzioni di configurazione disponibili per il gruppo utente SophosAdministrators. Per ulteriori informazioni su come riattivare il blocco rimozione, consultare la sezione [Riattivazione del blocco rimozione](#) a pagina 87.

9.2 Abilitazione del blocco rimozione

Importante: Se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Alla prima installazione di Sophos Endpoint Security and Control, il blocco rimozione è disabilitato. Se si è SophosAdministrator, è possibile abilitare il blocco rimozione.

Per abilitare il blocco rimozione:

1. Sulla **Home** page, sotto **Blocco rimozione**, cliccare su **Configura blocco rimozione**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nella finestra di dialogo **Configurazione blocco rimozione**, mettere la spunta nella casella **Attiva blocco rimozione**.
3. Cliccare su **Imposta** sotto la casella **Password**. Immettere e confermare una nuova password nella finestra di dialogo **Password del blocco rimozione**.

Suggerimento: La password deve contenere un minimo di otto caratteri, e devono essere presenti numeri e lettere maiuscole e minuscole.

9.3 Disabilitazione del blocco rimozione

Importante: Se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Se fate parte del gruppo SophosAdministrator siete autorizzati a disabilitare il blocco rimozione.

Disabilitazione del blocco rimozione:

1. Se non vi siete ancora autenticati, e l'opzione **Configura blocco rimozione** sulla **Home** page non è disponibile, seguite le istruzioni riportate nella sezione [Inserimento della password del blocco rimozione per configurare il software](#) a pagina 87 prima di passare alla fase 2.
2. Sulla **Home** page, sotto **Blocco rimozione**, cliccare su **Configura blocco rimozione**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
3. Nella finestra di dialogo **Configurazione blocco rimozione**, mettere o togliere la spunta nella casella **Attiva blocco rimozione** e cliccare su **OK**.

9.4 Riattivazione del blocco rimozione

Importante: Se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate. Se si appartiene al gruppo SophosAdministrator, è possibile riattivare il blocco rimozione.

Per riattivare il blocco rimozione:

1. Sulla **Home** page, sotto **Blocco rimozione**, cliccare su **Autenticare utente**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nella finestra di dialogo **Autenticazione blocco rimozione**, immettere la password del blocco rimozione e cliccare su **OK**.
3. Sulla **Home** page, sotto **Blocco rimozione**, cliccare su **Configura blocco rimozione**.
4. Nella finestra di dialogo **Configurazione blocco rimozione**, mettere la spunta nella casella **Attiva blocco rimozione**.

9.5 Password del blocco rimozione

Quando il blocco rimozione è attivo, è necessario immetterne la password se si desidera disattivare il blocco rimozione, o configurare la scansione in accesso e il rilevamento di comportamenti sospetti. È necessario essere membri del gruppo SophosAdministrator per fare ciò.

La password del blocco rimozione deve essere immessa solo dopo aver aperto Sophos Endpoint Security and Control. Se si chiude e poi si riapre Sophos Endpoint Security and Control, è necessario immettere nuovamente la password del blocco rimozione.

Se si desidera disinstallare uno dei componenti di Sophos Endpoint Security and Control, è necessario immettere la password del blocco rimozione prima di poter disabilitare il blocco rimozione e disinstallare il software.

Se il blocco rimozione è disattivato, ma la password del blocco rimozione è stata impostata in precedenza, è necessario inserire la password prima di riattivare il blocco rimozione.

Per abilitare il blocco rimozione è necessario immetterne la password, se:

- In precedenza si è abilitato il blocco rimozione, creata una password per esso, e poi lo si è disabilitato.
- Una password del blocco rimozione è stata creata nella console di gestione, ma il blocco rimozione non è attivo.

9.6 Inserimento della password del blocco rimozione per configurare il software

Se si appartiene al gruppo SophosAdministrator, è possibile autenticarsi inserendo la password del blocco rimozione.

Per autenticarsi:

1. Sulla **Home** page, sotto **Blocco rimozione**, cliccare su **Autenticare utente**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nella finestra di dialogo **Autenticazione blocco rimozione**, immettere la password del blocco rimozione e cliccare su **OK**.

9.7 Cambiamento della password del blocco rimozione

Importante: Se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

È necessario essere membri del gruppo SophosAdministrator per cambiare la password del blocco rimozione.

Per cambiare la password del blocco rimozione

1. Se non vi siete ancora autenticati, e l'opzione **Configura blocco rimozione** sulla **Home** page non è disponibile, seguite le istruzioni riportate nella sezione [Inserimento della password del blocco rimozione per configurare il software](#) a pagina 87 prima di passare alla fase 2.
2. Sulla **Home** page, sotto **Blocco rimozione**, cliccare su **Configura blocco rimozione**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
3. Nella finestra di dialogo **Configurazione del blocco rimozione**, cliccare su **Cambia** sotto la casella **Password**.
4. Immettere e confermare una nuova password nella finestra di dialogo **Password del blocco rimozione**.

Suggerimento: La password deve essere lunga almeno otto caratteri, e deve contenere numeri e lettere maiuscole e minuscole.

9.8 Disinstallazione del software di sicurezza Sophos

Se si appartiene al gruppo SophosAdministrator, è possibile disinstallare il software di sicurezza Sophos utilizzando il Pannello di Controllo:

- I componenti di Sophos Endpoint Security and Control (Sophos Anti-Virus, Sophos Client Firewall, Sophos AutoUpdate, Sophos Remote Management System).
- Sophos SafeGuard Disk Encryption

Per disinstallare il software di sicurezza Sophos quando è abilitato il blocco rimozione:

1. Sulla **Home** page, sotto **Blocco rimozione**, cliccare su **Autenticare utente**.
Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.
2. Nella finestra di dialogo **Autenticazione blocco rimozione**, immettere la password del blocco rimozione e cliccare su **OK**.
3. Sulla **Home** page, sotto **Blocco rimozione**, cliccare su **Configura blocco rimozione**.
4. Nella finestra di dialogo **Configurazione blocco rimozione**, mettere o togliere la spunta nella casella **Attiva blocco rimozione** e cliccare su **OK**.

Il blocco rimozione è disattivato.

5. Nel **Pannello di controllo**, aprire **Installazione applicazioni**, individuare il software che si desidera rimuovere e cliccare su **Cambia/Rimuovi** or **Rimuovi**. Seguire le istruzioni sullo schermo per disinstallare il software.

9.9 Visualizzazione del log del blocco rimozione:

Il log del blocco rimozione mostra due tipi di evento:

- Gli eventi di autenticazione del blocco rimozione riusciti; viene riportato il nome dell'utente autenticato e l'orario dell'autenticazione.
- I tentativi di sabotaggio falliti; dove vengono riportati i nomi dei componenti o dei prodotti Sophos oggetto di attacco, l'orario del tentativo e i dettagli dell'utente responsabile per tale tentativo.

È necessario essere membri del gruppo SophosAdministrator per visualizzare il log del blocco rimozione.

Visualizzazione del log del blocco rimozione:

- ❖ Sulla **Home** page, sotto **Blocco rimozione**, cliccare su **Visualizza log del blocco rimozione**. Per informazioni relative alla **Home** page, consultare la sezione [Home page](#) a pagina 4.

Dalla pagina log, è possibile copiare il log negli appunti, oppure inviarlo per e-mail o stamparlo.

Per trovare un testo specifico all'interno del log, cliccare su **Trova** e inserire il testo desiderato.

10 Risoluzione dei problemi

10.1 Aggiornamento non riuscito

10.1.1 Mancato funzionamento di un aggiornamento

Per ottenere maggiori dettagli sul mancato funzionamento degli aggiornamenti, controllare il log degli aggiornamenti; per ulteriori informazioni su come svolgere questa operazione, consultare la sezione [Visualizzazione del file di log degli aggiornamenti](#) a pagina 84.

Le sezioni seguenti spiegano la ragione per cui l'aggiornamento può non riuscire, e come modificare le impostazioni per risolvere il problema.

- [Sophos Endpoint Security and Control contatta la fonte sbagliata per gli aggiornamenti](#) a pagina 90
- [Sophos Endpoint Security and Control non riesce ad utilizzare il server proxy](#) a pagina 90
- [L'aggiornamento automatico non viene pianificato in modo corretto](#) a pagina 90
- [Il mantenimento della fonte degli aggiornamenti non viene curato](#) a pagina 91

10.1.2 Sophos Endpoint Security and Control contatta la fonte sbagliata per gli aggiornamenti

1. Nel menu **Configura**, cliccare su **Aggiornamento**.
2. Nella scheda **Percorso primario**, verificare che i dati relativi all'indirizzo e all'account siano quelli forniti dall'amministratore.
Per informazioni sulla configurazione del **Percorso primario**, consultare la sezione

10.1.3 Sophos Endpoint Security and Control non riesce ad utilizzare il server proxy

Se Sophos Endpoint Security and Control esegue l'aggiornamento via Internet, è necessario accertarsi che possa utilizzare un eventuale server proxy.

1. Nel menu **Configura**, cliccare su **Aggiornamento**.
2. Nella scheda **Percorso primario**, cliccare su **Dati proxy**.
3. Assicurarsi che l'indirizzo del server proxy, il numero della porta e i dati dell'account siano corretti.
Per informazioni su come inserire dati proxy, consultare la sezione

10.1.4 L'aggiornamento automatico non viene pianificato in modo corretto

1. Nel menu **Configura**, cliccare su **Aggiornamento**.

2. Cliccare sulla scheda **Pianificazione** (per informazioni sulla scheda **Operazione pianificata**, consultare la sezione [Pianificazione degli aggiornamenti](#) a pagina 82).
3. Se il computer è collegato alla rete, oppure se si esegue l'aggiornamento tramite una connessione Internet a banda larga, selezionare **Consenti aggiornamenti automatici** e inserire la frequenza di aggiornamento. Se si esegue l'aggiornamento tramite una connessione via modem, selezionare **Verifica la disponibilità di aggiornamenti in fase di connessione**.

10.1.5 Il mantenimento della fonte degli aggiornamenti non viene curato

La propria azienda potrebbe aver spostato la directory (sulla rete o su un server web) dalla quale si eseguono gli aggiornamenti. In alternativa, è possibile che l'azienda non curi affatto il mantenimento della directory.

Se si ritiene che sia proprio questo il caso, contattare l'amministratore di rete.

10.2 Minaccia non rimossa

Se Sophos Anti-Virus non ha rimosso una minaccia dal computer, la causa potrebbe essere una di quelle riportate qui di seguito.

La disinfezione automatica è disabilitata

Se Sophos Anti-Virus non ha tentato la disinfezione, verificare che la disinfezione automatica sia stata abilitata. Per informazioni su come abilitare la disinfezione automatica, consultare le seguenti sezioni:

- [Configurazione della disinfezione in accesso](#) a pagina 11
- [Configurazione della disinfezione dal menu del tasto destro del mouse](#) a pagina 20
- [Configurazione della disinfezione per una scansione personalizzata](#) a pagina 24

la rimozione automatica di adware e PUA non è disponibile per la scansione in accesso.

Disinfezione non riuscita

Se Sophos Anti-Virus non è riuscito a rimuovere una minaccia ("Disinfezione non riuscita"), è possibile che non riesca a rimuovere quel tipo di minaccia o che l'utente non possieda diritti di accesso sufficienti.

È necessaria una scansione completa del computer

Prima che Sophos Anti-Virus rimuova una minaccia multicomponente dal computer, o rilevi una minaccia nei file precedentemente nascosti, potrebbe essere necessario eseguire una scansione completa del computer per determinare tutti i componenti della minaccia.

1. Per eseguire una scansione di tutte le unità disco, inclusi i settori di avvio, eseguire la **Scansione del computer**. Per informazioni, consultare la sezione [Esecuzione della scansione completa del computer](#) a pagina 27.
2. Se la minaccia non è stata totalmente rilevata, la causa può risiedere in diritti di accesso dell'utente insufficienti o nel fatto che alcune unità o cartelle del computer, contenenti i componenti della minaccia, sono escluse dalla scansione. Per informazioni, consultare la

sezione [Aggiunta, modifica o cancellazione delle esclusioni per la scansione in accesso](#) a pagina 13. Controllare la lista degli oggetti esclusi dalla scansione. Se l'elenco contiene degli oggetti, rimuoverli e sottoporre di nuovo il computer a scansione.

L'unità rimovibile è protetta da scrittura

Se si tratta di un supporto rimovibile (per esempio un floppy disk o un CD), accertarsi che non sia protetto da scrittura.

Il volume NTFS è protetto da scrittura

In caso di file su un volume NTFS (Windows 2000 o successivo), accertarsi che questo non sia protetto da scrittura.

È stato segnalato un frammento di virus o spyware

Sophos Anti-Virus non rimuove i frammenti di virus/spyware perché non trova un'esatta corrispondenza con il virus/spyware. Consultare la sezione [Segnalato frammento di virus o spyware](#) a pagina 92.

10.3 Segnalato frammento di virus o spyware

Se viene segnalato un frammento di virus o spyware, fare quanto indicato di seguito:

1. Aggiornare immediatamente la protezione, in modo tale che Sophos Anti-Virus possieda i file di identità dei virus più recenti.
2. Eseguire la scansione completa del computer

■ [Aggiornamento immediato](#) a pagina 82

■ [Esecuzione della scansione completa del computer](#) a pagina 27

Se vengono segnalati ancora frammenti di virus o spyware, rivolgersi al supporto tecnico di Sophos per ricevere assistenza:

■ [Supporto tecnico](#) a pagina 104

La segnalazione di un frammento di virus o spyware indica che parte di un file corrisponde a parte di un virus o spyware. Le cause possibili sono tre.

Variante di un virus o spyware noto

Molti virus o spyware nuovi poggiano su esemplari esistenti, quindi frammenti di codice tipici di un virus o spyware noto possono sembrare parte di un nuovo codice. Se viene segnalato un frammento di virus o spyware, è possibile che Sophos Anti-Virus abbia rilevato un nuovo virus o spyware, che potrebbe diventare attivo.

Virus danneggiato

Molti virus contengono bug nelle loro routine di replicazione che fanno sì che questi virus infettino i file in modo non corretto. Una parte inattiva del virus (anche considerevole) potrebbe apparire all'interno del file che la ospita e venire rilevata da Sophos Anti-Virus. Un virus danneggiato non riesce a diffondersi.

Database contenente un virus o spyware

Quando si esegue una scansione completa del computer, Sophos Anti-Virus può segnalare la presenza di un frammento di virus o spyware all'interno di un file di database. In questo caso, non cancellare il database. Rivolgersi al supporto tecnico di Sophos per ricevere assistenza.

Per informazioni su come contattare il supporto tecnico, consultare la sezione [Supporto tecnico](#) a pagina 104.

10.4 Minaccia parzialmente rilevata

Per eseguire la scansione nel computer di unità disco, inclusi boot sector, eseguire la scansione completa del computer.

- [Esecuzione della scansione completa del computer](#) a pagina 27

Se la minaccia non è stata totalmente rilevata, la causa può risiedere nel fatto che alcune unità o cartelle del computer, contenenti i componenti della minaccia, sono escluse dalla scansione. Se nell'elenco delle esclusioni sono compresi alcuni di questi oggetti, rimuoverli ed eseguire nuovamente la scansione del computer.

- [Aggiunta, modifica o cancellazione delle esclusioni per la scansione su richiesta](#) a pagina 16

Se la minaccia non viene ancora completamente rilevata, la causa può risiedere in diritti di accesso dell'utente insufficienti.

Sophos Anti-Virus può non essere in grado di rilevare completamente o rimuovere le minacce i cui componenti sono installati in unità di rete.

10.5 Adware o PUA scomparsi dalla quarantena

Se un adware o PUA rilevato da Sophos Anti-Virus è scomparso dal Gestore quarantena, senza che sia stata prima eseguita un'azione su di esso, l'adware o PUA potrebbe essere stato autorizzato o rimosso dalla console di gestione o da un altro utente. Controllare la lista degli adware e PUA autorizzati per verificare se l'applicazione è stata autorizzata. Per maggiori informazioni su come effettuare tale operazione, consultare [Autorizzazione all'utilizzo di adware e PUA](#) a pagina 33.

10.6 Rallentamento del computer

Se il computer è diventato molto lento, è possibile che un'applicazione potenzialmente indesiderata (PUA) sia in esecuzione nel computer e lo stia monitorando. Se nel computer è abilitata la scansione in accesso, è possibile inoltre che compaiano molti allarmi sul desktop relativi a un'applicazione potenzialmente indesiderata (PUA). Per risolvere il problema, procedere nel modo seguente.

1. Eseguire la **Scansione del computer** per rilevare tutti i componenti dell'applicazione indesiderata (PUA). Per informazioni, consultare la sezione [Esecuzione della scansione completa del computer](#) a pagina 27.

Nota: Se, dopo la scansione, l'applicazione (PUA) è stata parzialmente rilevata, consultare [Minaccia parzialmente rilevata](#) a pagina 93, punto 2.

2. Rimuovere l'adware o PUA dal computer. Per maggiori informazioni su come effettuare tale operazione, consultare [Gestione di adware e PUA in quarantena](#) a pagina 38.

10.7 Accesso alle unità con settore di avvio infetti

Importante: se viene utilizzata una console di gestione per amministrare Sophos Endpoint Security and Control su questo computer, essa potrebbe ignorare le modifiche qui apportate.

Per impostazione predefinita, Sophos Anti-Virus impedisce l'accesso ai supporti rimovibili i cui settori di avvio sono infetti.

Per consentire l'accesso (per es. per copiare file da un floppy infetto da un virus del boot sector):

1. Cliccare su **Inizio > Anti-virus e HIPS (Sistema di prevenzione delle intrusioni su host) > Configurazione di antivirus e HIPS > Configurazione > scansione in accesso scansione** .
2. Nella scheda **Scansione**, selezionare la casella di spunta **Consenti accesso alle unità con boot sector infetti**.

Importante: appena terminato l'accesso al disco, deselezionare la casella di spunta e rimuovere il disco dal computer, in modo tale che non provi a infettare nuovamente il computer al momento del riavvio.

10.8 Impossibile accedere ad alcune aree di Sophos Endpoint Security and Control

Se non si riesce a utilizzare o a configurare determinate aree di Sophos Endpoint Security and Control, ciò può essere dovuto al fatto che l'accesso a queste aree sia riservato ai membri di particolari gruppi di utenti Sophos.

Per ulteriori informazioni sui gruppi di utenti Sophos, consultare la sezione [Gruppi Sophos](#) a pagina 5.

10.9 Rimozione degli effetti secondari dei virus

La rimozione degli effetti secondari dei virus dipende dal modo in cui il virus ha infettato il computer.

Effetti secondari del virus

Alcuni virus non provocano effetti secondari, altri possono avere degli effetti secondari così gravi che è necessario ripristinare l'hard disk.

Alcuni virus alterano i dati gradualmente. Questo tipo di alterazione può essere difficile da rilevare.

Cosa fare

È molto importante leggere l'analisi del virus sul sito web di Sophos e verificare con attenzione i documenti dopo aver effettuato la disinfezione. Consultare [Informazioni sulla disinfezione](#) a

pagina 43 per sapere come visualizzare, sul sito web di Sophos, i dettagli sugli effetti secondari dei virus.

È essenziale disporre di copie di backup attendibili. Se non si disponeva di tali copie prima dell'infezione, è necessario cominciare a crearle e conservarle in caso di future infezioni.

Talvolta è possibile recuperare i dati dai dischi danneggiati da un virus. Sophos fornisce delle utilità per la riparazione dei danni causati da alcuni virus.

Rivolgersi al supporto tecnico di Sophos per ricevere assistenza.

Per informazioni su come contattare il supporto tecnico, consultare la sezione [Supporto tecnico](#) a pagina 104.

10.10 Rimozione degli effetti secondari di adware e PUA

La rimozione di adware e PUA può comportare alcuni effetti secondari che non possono essere eliminati durante la disinfezione.

Il sistema operativo è stato modificato

Alcuni adware e PUA modificano il sistema operativo Windows, per esempio cambiano le impostazioni della connessione Internet. Sophos Sophos Anti-Virus non può sempre ripristinare tutte le impostazioni con i valori precedenti all'installazione dell'adware/PUA. Se, per esempio, un adware o PUA ha modificato la pagina iniziale del browser, Sophos Sophos Anti-Virus

Utilità non rimosse

Alcuni adware e PUA possono installare nel computer delle utilità come i file .dll o .ocx. Se un'utilità è innocua (vale a dire, se non possiede le caratteristiche di adware e PUA), per esempio una libreria della lingua, e non è integrata nell'adware o PUA, Sophos Sophos Anti-Virus può non rilevarla come componente dell'adware o PUA stesso. In questo caso, il file non viene rimosso dal computer neanche dopo la rimozione dell'adware o PUA che l'ha installato.

L'adware o PUA fa parte di un programma necessario

Talvolta un oggetto, adware o PUA, fa parte di un programma installato intenzionalmente, ed è necessario affinché il programma funzioni correttamente. Se si rimuove l'adware o PUA, il programma potrebbe non venire più eseguito nel computer.

Cosa fare

È molto importante leggere l'analisi della minaccia sul sito web di Sophos. Per scoprire come visualizzare sul sito web di Sophos i dettagli sugli effetti secondari di adware o PUA, consultare la sezione [Informazioni sulla disinfezione](#) a pagina 43.

Per poter ripristinare il sistema e le sue impostazioni allo stato preesistente, è necessario eseguire periodicamente il backup del sistema. È inoltre necessario eseguire copie di backup dei file eseguibili originali dei programmi che si desidera utilizzare.

Per ulteriori informazioni o consigli sulla rimozione degli effetti secondari di adware e PUA, rivolgersi al supporto tecnico di Sophos.

Per informazioni su come contattare il supporto tecnico, consultare la sezione [Supporto tecnico](#) a pagina 104.

10.11 Segnalato errore della password

Se si cerca di pianificare una scansione personalizzata e viene visualizzato un messaggio di errore relativo alla password, assicurarsi che:

- La password sia quella relativa all'account utente
- La password non sia vuota

Per assicurarsi che la password sia corretta, verificare le proprietà dell'account utente in **Account utente**, nel **Pannello di controllo**.

10.12 Messaggio di errore "Service failure"

Sintomi

Nell'area di notifica viene visualizzato uno dei seguenti messaggi di errore:

- Antivirus e HIPS: errore del servizio
- Firewall: errore del servizio

Cause

Si è verificato un errore in uno dei servizi di Sophos Endpoint Security and Control e il computer deve essere riavviato.

Risoluzione del problema

1. Tramite Windows, aprire Servizi.
2. Effettuare una delle seguenti operazioni:
 - Se viene visualizzato il messaggio d'errore **Antivirus e HIPS: errore del servizio**, cliccare col tasto destro del mouse su **Sophos Anti-Virus** e quindi su **Riavvia**.
 - Se viene visualizzato il messaggio d'errore **Firewall: errore del servizio**, cliccare col tasto destro del mouse su **Sophos Client Firewall** e quindi su **Riavvia**.

Note

- Per aprire Servizi, cliccare su **Start**, successivamente su **Pannello di controllo**, cliccare due volte su **Strumenti di amministrazione** e poi due volte su **Servizi**.

10.13 Il database del log firewall è danneggiato

Sintomi

Mentre si utilizza il visualizzatore del log firewall, compare il messaggio di errore: "L'attuale database del log di Sophos Client Firewall è danneggiato".

Causa

Il database del log eventi del firewall si è danneggiato, ed ha bisogno di essere ricreato.

Risoluzione del problema

Per svolgere le seguenti operazioni, è necessario essere membri del gruppo Windows Administrators sul computer in questione.

1. Tramite Windows, aprire Servizi.
2. Cliccare col tasto destro del mouse su **Sophos Client Firewall** Manager, e quindi su **Arresta**.
3. Mediante Windows Explorer, andare su C:\Documents and Settings\All Users\Application Data\Sophos\Sophos Client Firewall\logs.

Per visualizzare questa cartella nascosta, può essere necessario impostare in Windows Explorer la visualizzazione di file e cartelle nascosti.

4. Cancellare op_data.mdb.
5. In "Servizi", cliccare con il tasto destro del mouse su **Sophos Client Firewall** Manager, e poi su **Riavvia**.

Note

- Per aprire Servizi, cliccare su **Start**, successivamente su **Pannello di controllo**, cliccare due volte su **Strumenti di amministrazione** e poi due volte su **Servizi**.

11 Glossario

Adware e PUA	L'adware prevede la presentazione all'utente di messaggi pubblicitari, quali messaggi popup, che incidono sulla produttività degli utenti e sull'efficienza del sistema. Un'applicazione potenzialmente indesiderata (PUA) è un'applicazione che di per sé non è malevola, ma viene generalmente considerata inadatta per la maggior parte delle reti aziendali.
Analisi del comportamento in fase di esecuzione	Analisi dinamica svolta tramite il rilevamento del comportamento sospetto e del buffer overflow.
applicazione attendibile	Applicazione a cui è concesso accesso alla rete completo e incondizionato.
applicazione controllata	Un'applicazione la cui esecuzione nel computer è impedita dai criteri di sicurezza aziendali.
Applicazioni bloccate	Stato che indica la negazione dell'accesso alla rete ad applicazioni (inclusi i processi nascosti), connessioni, protocolli, messaggi ICMP ecc.
Barra delle descrizioni	Barra del visualizzatore del log che si trova sopra la vista dei dati e che contiene il nome dell'elemento della vista ad albero selezionato.
blocco rimozione	Una funzione che impedisce a malware noto e utenti non autorizzati (amministratori locali e utenti con conoscenze tecniche limitate), la disinstallazione del software di sicurezza Sophos o la disabilitazione tramite interfaccia di Sophos Endpoint Security and Control.
Checksum	Ogni versione di un'applicazione ha un checksum unico. Il firewall può utilizzare tale checksum per decidere se un'applicazione è consentita o meno.
Configurazione primaria	La configurazione del firewall utilizzata per la rete aziendale a cui l'utente si collega per svolgere il suo lavoro giornaliero.
Configurazione secondaria	La configurazione del firewall utilizzata quando gli utenti non sono connessi alla rete aziendale primaria, ma a una rete differente, quale la rete wireless di un hotel o aeroporto, oppure un'altra rete aziendale.
content Control List (CCL)	Un set di condizioni che specificano il contenuto di un file, per esempio numeri di carte di credito o debito (bancomat) o conti corrente bancari simili ad altri tipi di dati che possono portare

all'identificazione personale. Esistono due tipi di Content Control List: SophosLabs Content Control List e Content Control List personalizzata.

controllo dati	Funzione che riduce il rischio di perdita di dati accidentale dalle workstation. Questa funzione entra in azione quando l'utente di una workstation tenta di trasferire un file che soddisfa i parametri stabiliti da criteri e regole di controllo dei dati. Per esempio quando un utente cerca di copiare in un dispositivo di memorizzazione removibile un foglio elettronico contenente dati relativi ai clienti o cerca di caricare un documento contrassegnato come confidenziale in un account di web mail; in questi casi la funzione di controllo dei dati, se configurata in tal senso, bloccherà il trasferimento.
controllo dispositivi	Funzione che riduce la perdita accidentale di informazioni dalle workstation e che limita l'introduzione di software esterni alla rete. Entra in azione quando l'utente di una workstation tenta di utilizzare nella propria workstation dispositivi di memorizzazione o di rete non autorizzati.
Corrispondenza	Equivale al contenuto definito in un Content Control List.
Criteri firewall	Impostazioni volute dalla console di gestione e che il firewall utilizza per monitorare la connessione del computer a Internet e ad altre reti.
Disinfezione	La disinfezione elimina le minacce presenti nel computer rimuovendo i virus da file e boot sector, spostando o cancellando un file sospetto, o cancellando un oggetto adware o PUA. Non è disponibile per le minacce rilevate tramite la scansione della pagina web perché le minacce non vengono scaricate nel computer. Pertanto, in tali casi non è necessaria alcuna azione.
Disinfezione automatica	Disinfezione svolta senza l'intervento o il consenso dell'utente.
Disinfezione manuale	Disinfezione svolta tramite utilità di disinfezione specifiche o cancellando i file manualmente.
Dispositivi di memorizzazione	Dispositivi di memorizzazione rimovibili (per es. unità USB flash, lettori di schede per PC e unità hard disk USB), unità CD/DVD, unità floppy disk e dispositivi di memorizzazione rimovibili sicuri (per es. unità SanDisk Cruzer Enterprise, Kingston Data Traveller, IronKey Enterprise e IronKey Basic USB flash con cifratura dell'hardware).

Errore della scansione	Errore verificatosi durante la scansione di un file, per esempio quando viene negato l'accesso.
Evento firewall	Situazione che si verifica nel computer quando un'applicazione sconosciuta, o il sistema operativo, prova a comunicare con un altro computer tramite connessione di rete in una modalità non specificamente richiesta dalle applicazioni in esecuzione nel computer ricevente.
Evento minaccia	Rilevamento o disinfezione di una minaccia.
file di identità del virus (IDE)	File che consente a Sophos Anti-Virus di rilevare e rimuovere un determinato virus, trojan o worm.
file sospetto	File che presenta una serie di caratteristiche comunemente, ma non esclusivamente, riscontrate in virus.
Finestra di apprendimento	Una finestra di dialogo che chiede all'utente di scegliere se consentire o bloccare l'attività di rete quando un'applicazione sconosciuta richiede l'accesso alla rete.
Gestore autorizzazioni	Il modulo che consente di autorizzare adware e PUA, file sospetti, applicazioni sospette o buffer overflow.
Gestore quarantena	Il modulo che consente di visualizzare e gestire gli elementi messi in quarantena.
Host Intrusion Prevention System (HIPS)	Termine generale che indica l'analisi del comportamento prima dell'esecuzione ed in fase di esecuzione.
ICMP	Acronimo di "Internet Control Message Protocol". Un protocollo del livello di rete che fornisce la correzione di errori e altre informazioni relative all'elaborazione dei pacchetti IP.
Impostazioni cancellazione log	Impostazioni che controllano quando i dati vengono cancellati.
Impostazioni ICMP	Le impostazioni che determinano quali tipi di comunicazione di gestione della rete sono consentiti.
Impostazioni processo	Impostazioni che determinano se a processi modificati o nascosti debba essere concesso accesso alla rete.
Ispezione di stato	Tecnologia firewall che consente di aggiornare la tabella relativa alle connessioni di rete TCP e UDP attive. Il firewall consentirà l'accesso solo ai pacchetti che soddisfano uno stato di connessione noto; tutti gli altri verranno rifiutati.

Memoria di sistema	Memoria che funge da ponte fra le applicazioni e l'elaborazione dei dati svolta a livello di hardware. Viene utilizzata dal sistema operativo.
Messaggistica istantanea	Categoria di applicazioni controllate che comprende applicazioni di messaggistica istantanea (per es. MSN).
Modalità di funzionamento	Impostazione che stabilisce se il firewall agisce in base all'input da parte dell'utente (modalità interattiva) o automaticamente (modalità non interattive).
Modalità interattiva	La modalità in cui il firewall visualizza una o più finestre di apprendimento quando viene rilevato traffico di rete per cui non esiste alcuna regola.
Modalità non interattiva	Modalità in cui il firewall consente o blocca tutto il traffico di rete per cui non è stata rilevata alcuna regola.
NetBIOS	Acronimo di "Network Basic Input/Output System". Software che fornisce un'interfaccia tra il sistema operativo, il bus di I/O e la rete. Quasi tutte le LAN basate su Windows sono basate su NetBIOS.
Processo nascosto	Un'applicazione a volte ne avvia un'altra che svolga delle operazioni di accesso alla rete per lei. Applicazioni malevole possono utilizzare questa tecnica per aggirare i firewall; possono infatti lanciare un'applicazione ritenuta affidabile per accedere alla rete invece che tentare da sole.
Protocollo di rete	Set di regole o standard progettati per consentire ai computer di connettersi tramite la rete e di scambiare informazioni col minor margine di errore possibile.
Raw socket	I raw socket consentono ai processi di controllare tutti gli aspetti dei dati che inviano in rete e possono essere utilizzati per scopi malevoli.
Regola con elevata priorità	Regola applicata prima di qualsiasi regola globale o di applicazione.
regola dei contenuti	Regola comprendente una o più Content Control List e indicante l'azione da intraprendere se l'utente cerca di trasferire in una destinazione specificata i dati che soddisfano tutte le Content Control List presenti nella regola.
Regola dell'applicazione	Una regola applicabile solo a pacchetti di dati trasferiti attraverso la rete a o da una particolare applicazione.

Regola di sistema	Regola applicata a tutte le applicazioni che consentirà o bloccherà le attività di rete di livello basso.
Regola personalizzata	Regola creata dall'utente per indicare le circostanze in cui l'esecuzione di un'applicazione è consentita.
Regole globali	Regole applicate a tutte le connessioni di rete e applicazioni non ancora in possesso di regole specifiche. Hanno priorità minore delle regole impostate nella pagina della LAN. Hanno priorità minore anche delle regole delle applicazioni (a meno che non diversamente indicato dall'utente).
Rilevamento di buffer overflow	Rileva attacchi di buffer overflow.
Rilevamento di comportamento sospetto	Analisi dinamica del comportamento di tutti i programmi in esecuzione sul sistema al fine di rilevare e bloccare le attività che appaiono malevole.
Rootkit	Trojan o tecnologia utilizzata per nascondere la presenza di un oggetto malevolo (processo, file, chiave di registro o porta di rete) all'utente del computer o all'amministratore.
Scansione completa	Scansiona tutte le parti di ciascun file.
Scansione dal menu del tasto destro del mouse	Scansione di file in Windows Explorer o nel desktop eseguiti tramite menu.
Scansione in accesso	Il vostro principale metodo di protezione contro virus. Ogni qual volta si accede a un file (copia, salva, sposta o apri), Sophos Anti-Virus ne esegue la scansione e ne consente l'accesso solo se tale file non costituisce una minaccia per il computer.
Scansione normale	Scansiona solo le parti del file con maggiori probabilità di essere infettate da virus.
scansione pianificata	Scansione del computer, o di parti di esso, eseguita ad orari fissi.
scansione su richiesta	Scansione avviata dall'utente. È possibile utilizzare la scansione su richiesta per sottoporre a scansione qualsiasi elemento, da un solo file a tutto ciò che è contenuto nel proprio computer e per cui si dispone di autorizzazione per la lettura.
Sophos Live Protection	Funzione che utilizza la tecnologia "in-the-cloud" per decidere all'istante se un file sospetto rappresenta una minaccia e intraprendere l'azione specificata nella configurazione di disinfezione di Sophos Anti-Virus.

Spyware	Programma che si autoinstalla nel computer di un utente utilizzando sotterfugi o tecniche di ingegneria sociale, per poi inviare informazioni da quel computer a terzi, senza il consenso dell'utente o a sua insaputa.
tipo file true	Il tipo di file che viene verificato tramite l'analisi della sua struttura piuttosto che dell'estensione del nome. Si tratta di un metodo più affidabile.
Traffico sconosciuto	Forma di accesso alla rete da parte di un'applicazione o servizio per cui il firewall non ha rilevato alcuna regola.
virus non identificato	Virus per il quale non esiste uno specifico file di identità.
Vista ad albero	Vista che controlla quali dati il visualizzatore di log mostra nella propria vista dei dati.
Vista dati	Vista che mostra dati diversi a seconda dell'elemento della vista ad albero selezionato.
visualizzatore del log	Visualizzazione dei dati relativi agli eventi del database quali connessioni consentite o bloccate, il log di sistema e tutti gli allarmi che sono stati generati.
Voice over IP	Categoria di applicazioni controllate che comprende applicazioni di Voice over IP.

12 Supporto tecnico

È possibile ricevere supporto tecnico per i prodotti Sophos in uno dei seguenti modi:

- Visitando la community SophosTalk su <http://community.sophos.com/> e cercando altri utenti con lo stesso problema.
- Visitando la knowledge base del supporto Sophos su <http://www.sophos.it/support/>.
- Scaricando la documentazione del prodotto su <http://www.sophos.it/support/docs/>.
- Inviando un'e-mail a support@sophos.com, indicando il o i numeri di versione del software Sophos in vostro possesso, i sistemi operativi e relativi livelli di patch, ed il testo di ogni messaggio di errore.

13 Note legali

Copyright © 2011 Sophos Limited. Tutti i diritti riservati. Nessuna parte di questa pubblicazione può essere riprodotta, memorizzata in un sistema di recupero informazioni, o trasmessa, in qualsiasi forma o con qualsiasi mezzo, elettronico o meccanico, inclusi le fotocopie, la registrazione e altri mezzi, salvo che da un licenziatario autorizzato a riprodurre la documentazione in conformità con i termini della licenza, oppure previa autorizzazione scritta del titolare dei diritti d'autore.

Sophos e Sophos Anti-Virus sono marchi registrati di Sophos Limited. Tutti gli altri nomi citati di società e prodotti sono marchi o marchi registrati dei rispettivi titolari.

Common Public License

Il software Sophos descritto in questo documento comprende o può comprendere programmi di software concessi in licenza (o sottolicenza) all'utente secondo i termini della Common Public License (CPL), la quale, tra gli altri diritti, permette all'utente di avere accesso al codice sorgente. La CPL richiede, per qualsiasi software concesso in licenza secondo i termini della stessa, e distribuito in formato codice oggetto, che il codice sorgente di tale software venga messo a disposizione anche degli altri utenti del formato codice oggetto. Per qualsiasi software che rientri nei termini della CPL, il codice sorgente è disponibile tramite ordine postale inviandone richiesta a Sophos; per e-mail a support@sophos.com o tramite internet su <http://www.sophos.it/support/queries/enterprise.html>. Una copia dei termini per tali software è reperibile all'indirizzo <http://opensource.org/licenses/cpl1.0.php>

ConvertUTF

Copyright 2001–2004 Unicode, Inc.

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

OpenSSL cryptographic toolkit

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL license

Copyright © 1998-2011 The OpenSSL Project. Tutti i diritti riservati.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (ey@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

Copyright © 1995–1998 Eric Young (ey@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (ey@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word "cryptographic" can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

Indice

A

- abilitazione della scansione in accesso 10
- abilitazione finestre di apprendimento su checksum 63
- accesso ai dischi 8, 94
- adware 93, 95
 - autorizzazione 33
 - Disinfezione automatica 20, 24
 - ricerca di 8, 19, 22
- adware autorizzati, blocco 33
- adware in quarantena, gestione 38
- aggiornamento 82, 84, 90
- aggiornamento immediato 82
- aggiornamento tramite connessione dial-up 82
- aggiunta utenti ai gruppi Sophos 6
- Analisi del comportamento in fase di esecuzione 15, 28
- Analisi delle minacce 43
- antivirus
 - configurazione del log eventi 46
 - configurazione della messaggistica SNMP 46
 - configurazione di allarmi tramite e-mail 44
 - configurazione messaggistica desktop 44
- applicazioni
 - autorizzazione 57
 - blocco 58
 - utilizzo per l'autenticazione di 72
- applicazioni controllate
 - autorizzazione 41
 - gestione 41
 - ricerca di 32
- autenticazione di applicazioni, utilizzo di checksum per 72
- autorizzazione
 - adware 33
 - applicazioni 57
 - applicazioni controllate 41
 - browser web 55
 - buffer overflow 34, 40
 - comportamento sospetto 34, 40
 - condivisione stampanti 56–57
 - download del FTP 55
 - e-mail 54
 - file sospetti 34
 - processi nascosti 71

- autorizzazione (*continua*)

- PUA 33
- raw socket 72
- siti web 34
- traffico LAN 55

B

- blocco
 - adware autorizzati 33
 - applicazioni 58
 - condivisione stampanti 57
 - PUA autorizzate 33
 - siti web malevoli 32
- blocco rimozione
 - abilitazione 86
 - attivazione 86
 - autenticazione utente 87
 - come cambiare la password 88
 - configurazione del software 87
 - disabilitazione 86
 - disattivazione 86
 - disinstallazione del software di sicurezza Sophos 88
 - Disinstallazione di Sophos Endpoint Security and Control 88
 - immissione della password 87
 - log 89
 - panoramica 85
 - riattivazione 87
- boot sector infetto 8, 94
- browser web, autorizzazione 55
- buffer overflow
 - autorizzazione 34, 40
 - rilevamento 30

C

- cancellazione scansioni personalizzate 27
- checksum, utilizzo per l'autenticazione di applicazioni 72
- comportamento malevolo
 - rilevamento 29
- comportamento sospetto
 - autorizzazione 34, 40
 - rilevamento 29
- comportamento sospetto in quarantena, gestione 40
- computer lento, risoluzione dei problemi 93

condivisione file e stampanti, autorizzazione 56–57
 condivisione file e stampanti, blocco 57
 condivisione file, autorizzazione 56–57
 condivisione file, blocco 57
 condivisione stampanti, autorizzazione 56–57
 condivisione stampanti, blocco 57
 configurazione

- reportistica centrale 75
- allarmi antivirus tramite e-mail 44
- diritti utente per Gestore quarantena 6
- Log del firewall 78
- log della scansione 47
- log eventi dell'antivirus 46
- messaggistica desktop relativa all'antivirus 44
- messaggistica SNMP relativa all'antivirus 46
- scansione dal menu del tasto destro del mouse 19
- scansione in accesso 8
- scansioni personalizzate 22

 configurazioni secondarie

- creazione 74

 controllo dati, disabilitazione temporanea 51
 Controllo dispositivi 49

- blocco bridging di rete 49
- dispositivi controllati 49

 creazione di scansioni personalizzate 21

D

diritti di accesso 5, 94
 diritti utente 5, 94
 diritti utente per Gestore quarantena, configurazione 6
 disabilitazione del firewall 54
 Disabilitazione della scansione 49
 disabilitazione della scansione alla ricerca di applicazioni controllate 33
 disabilitazione della scansione in accesso 10
 disinfezione 91
 Disinfezione

- Informazioni su 42
- Risoluzione dei problemi 91

 Disinfezione automatica

- adware 20, 24
- file sospetti 11, 20, 24
- PUA 20, 24
- Spyware 11, 20, 24
- virus 11, 20, 24

disinstallazione del software di sicurezza Sophos 88
 download del FTP, autorizzazione 55
 Due schede di rete

- utilizzo 73

E

e-mail, autorizzazione di 54
 effetti secondari 95
 errore della password 96
 esclusione di oggetti dalla scansione in accesso 13
 esclusione di oggetti dalla scansione su richiesta 16
 esecuzione della scansione dal menu del tasto destro del mouse 21
 esecuzione di scansioni complete di computer 27
 esecuzione di scansioni personalizzate 26
 Esegui scansione a priorità più bassa" 22
 esportazione di file di configurazione firewall 64
 esportazione di tutti i record dal visualizzatore del log del firewall 80

F

file checksum scansionati, ripristino 12
 file di archivio, scansione 8, 19, 22
 file di configurazione firewall

- esportazione 64
- importazione 64

 file sospetti

- autorizzazione 34
- Disinfezione automatica 11, 20, 24
- ricerca di 8, 19, 22

 file sospetti in quarantena, gestione 39
 filtraggio dei messaggi ICMP 59
 filtraggio dei record 80
 finestre di apprendimento sui checksum

- abilitazione 63
- Modalità interattiva 62

 firewall

- disabilitazione 54

 Frammento 91

G

gestione delle applicazioni controllate 41
 gestione di adware in quarantena 38
 gestione di comportamento sospetto in quarantena 40
 gestione di file sospetti in quarantena 39

- gestione di PUA in quarantena 38
- Gestione di spyware in quarantena 37
- gestione di virus in quarantena 37
- Gestore quarantena 35
- gruppi di utenti 5, 94
- Gruppi Sophos 5
 - Aggiunta di utenti 6

H

- HIPS (Sistema di prevenzione delle intrusioni su host) 28
- Home page 4
- Host Intrusion Prevention System (Sistema di prevenzione delle intrusioni su host) 28

I

- icona nell'area di notifica 90
- icone
 - oggetti da esaminare 22
- importazione di file di configurazione firewall 64
- impostazione delle regole globali 67, 69, 71
- impostazione di una regola 68–69
- informazioni sulla disinfezione 43
- Informazioni sulla disinfezione 43
- Informazioni sulla sicurezza 43
- Introduzione
 - cosa fare per prima cosa 53

L

- larghezza di banda utilizzata per gli aggiornamenti, limitazione 84
- limitazione della larghezza di banda utilizzata per gli aggiornamenti 84
- log degli aggiornamenti 84
- Log del firewall
 - configurazione 78
- log della scansione
 - configurazione 47
 - visualizzazione 48
- log della scansione personalizzata
 - visualizzazione 27

M

- memoria di sistema, scansione 8, 22
- messaggi ICMP
 - filtraggio 59

- messaggi ICMP (*continua*)
 - informazioni su 59
- minaccia parzialmente rilevata 93
- modalità di funzionamento, cambia a interattiva 60
- Modalità interattiva
 - finestre di apprendimento sui checksum 62
 - messaggi su applicazioni 62
 - messaggi su raw socket 62
 - messaggi sui processi nascosti 61
 - messaggi sul protocollo 62
- modalità interattiva, abilitazione 60
- modalità interattiva, info su 60
- modalità non interattiva, cambia con 61
- monitoraggio del comportamento 28
 - abilitazione 15, 28

O

- oggetti sospetti, preautorizzazione 34

P

- percorsi primari
 - definizione 74
- pianificazione degli aggiornamenti 82
- pianificazione di una scansione 96
- pianificazione di una scansione personalizzata 25
- preautorizzazione di oggetti sospetti 34
- priorità regole 64
- priorità, scansione 22
- processi nascosti, autorizzazione 71
- PUA 93, 95
 - autorizzazione 33
 - Disinfezione automatica 20, 24
 - ricerca di 8, 19, 22
- PUA autorizzate, blocco 33
- PUA in quarantena, gestione 38

R

- raw socket, autorizzazione 72
- record del log
 - filtraggio 80
- Regola
 - impostazione 68–69
- Regole globali
 - impostazione 67, 69, 71
- regole globali predefinite
 - ulteriori informazioni 66

reportistica centrale, configurazione 75
ricerca di adware e PUA 8, 19, 22
ricerca di file sospetti 8, 19, 22
ricerca di virus di Mac 8
riconoscimento presenza
 creazione di configurazioni secondarie 74
 definizione dei percorsi primari 74
 Informazioni su 73
 Utilizzo di due schede di rete 73
rilevamento di buffer overflow 30
rilevamento di comportamento malevolo 29
rilevamento di comportamento sospetto 29
rilevamento parziale 93
Rimozione degli effetti secondari di una minaccia 95
rinomina scansioni personalizzate 26
ripristino dei file checksum scansionati 12
rootkit, ricerca 22

S

scansione alla ricerca di applicazioni controllate, disabilitazione 33
scansione alla ricerca di rootkit 22
scansione dal menu del tasto destro del mouse 21
scansione dal menu del tasto destro del mouse, configurazione 19
scansione dal menu del tasto destro del mouse, esecuzione 21
scansione dei file di archivio 8, 19, 22
scansione della memoria di sistema 8, 22
scansione di singoli oggetti 21
scansione di tutti i file 8, 19, 22
scansione di un singolo oggetto 21
scansione in accesso
 abilitazione 10
 configurazione 8
 disabilitazione 10
 esclusione di oggetti dalla 13
 specificazione delle estensioni dei file 12
scansione in accesso e su richiesta, differenze 8
scansione per la ricerca di applicazioni controllate 32
scansione su richiesta
 esclusione di oggetti dalla 16
 specificazione delle estensioni dei file 16
scansione su richiesta, tipi di 15
scansioni complete di computer, esecuzione 27
scansioni personalizzate
 configurazione 22

scansioni personalizzate (*continua*)
 creazione 21
 esecuzione 26
 pianificazione 25
 rimozione 27
 rinomina 26
Segnalato frammento, risoluzione dei problemi 92
server primario 82
server proxy 83
server secondario 83
siti web
 autorizzazione 34
siti web malevoli
 Protezione 32
Sophos Endpoint Security and Control 3
Sophos Live Protection
 abilitazione 31
 attivazione 31
 disabilitazione 31
 disattivazione 31
 log 31
 panoramica 30
 tecnologia in-the-cloud 30
sospensione della scansione 49
specificazione delle estensioni dei file per la scansione in accesso 12
Spyware
 Disinfezione automatica 11, 20, 24
spyware in quarantena, gestione 37

T

tecnologia in-the-cloud 30
tipi di scansione su richiesta 15
traffico LAN, autorizzazione 55
tutti i file, scansione 8, 19, 22

V

virus
 Disinfezione automatica 11, 20, 24
 Rimozione degli effetti secondari di una minaccia 94
virus di Mac, ricerca 8
virus in quarantena, gestione 37
visualizzatore del log
 Informazioni su 77
visualizzatore del log firewall
 esportazione record 80

visualizzazione

log della scansione 48

log della scansione personalizzata 27

W

Web Protection

panoramica 32